

Configuración de la autenticación de AD para clientes AnyConnect

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama y escenario de la red](#)

[Configuraciones de Active Directory](#)

[Determinar DN Base LDAP y DN de Grupo](#)

[Creación de una cuenta de FTD](#)

[Crear grupos de AD y agregar usuarios a grupos de AD \(opcional\)](#)

[Copiar la raíz del certificado SSL LDAPS \(solo se requiere para LDAPS o STARTTLS\)](#)

[Configuraciones de FMC](#)

[Verificar licencia](#)

[Rango de configuración](#)

[Configuración de AnyConnect para la autenticación de AD](#)

[Habilitar la política de identidad y configurar las políticas de seguridad para la identidad del usuario](#)

[Configurar exención de NAT](#)

[Implementación](#)

[Verificación](#)

[Configuración final](#)

[Configuración AAA](#)

[Configuración de AnyConnect](#)

[Conexión con AnyConnect y verificación de las reglas de la política de control de acceso](#)

[Verificar con eventos de conexión FMC](#)

[Troubleshoot](#)

[Depuraciones](#)

[Depuraciones de LDAP en funcionamiento](#)

[No se puede establecer una conexión con el servidor LDAP](#)

[Enlace DN de inicio de sesión o contraseña incorrecta](#)

[El servidor LDAP no puede encontrar el nombre de usuario](#)

[Contraseña incorrecta para el nombre de usuario](#)

[Prueba AAA](#)

[Capturas de paquetes](#)

[Registros del Visor de sucesos de Windows Server](#)

Introducción

Este documento describe cómo configurar la autenticación de Active Directory (AD) para los clientes de AnyConnect que se conectan a Firepower Threat Defence (FTD).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de red privada virtual (VPN) de RA en Firepower Manage Center (FMC)
- Configuración del servidor de protocolo ligero de acceso a directorios (LDAP) en FMC
- Active Directory (AD)
- Nombre de dominio completo (FQDN)
- Intersight Infrastructure Services (IIS)
- Protocolo de escritorio remoto (RDP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft 2016 Server
- FMCv con 6.5.0
- FTDv con 6.5.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento describe cómo configurar la autenticación de Active Directory (AD) para los clientes de AnyConnect que se conectan a Firepower Threat Defense (FTD), administrado por Firepower Management Center (FMC).

La identidad del usuario se utiliza en las políticas de acceso para restringir a los usuarios de AnyConnect a direcciones IP y puertos específicos.

Configurar

Diagrama y escenario de la red



Windows Server está preconfigurado con IIS y RDP para probar la identidad del usuario. En esta guía de configuración, se crean tres cuentas de usuario y dos grupos.

Cuentas de usuario:

- Administrador de FTD: se utiliza como cuenta de directorio para permitir que el FTD se enlace al servidor de Active Directory.
- Administrador de TI: cuenta de administrador de prueba utilizada para demostrar la identidad del usuario.
- Usuario de prueba: cuenta de usuario de prueba utilizada para demostrar la identidad del usuario.

Grupos:

- Administradores de AnyConnect: grupo de prueba que se agrega al administrador de TI para demostrar la identidad del usuario. Este grupo solo tiene acceso RDP al servidor Windows Server.
- Usuarios de AnyConnect: grupo de prueba que se agrega para demostrar la identidad del usuario. Este grupo sólo tiene acceso HTTP al servidor Windows Server.

Configuraciones de Active Directory

Para configurar correctamente la autenticación de AD y la identidad del usuario en FTD, se requieren algunos valores.

Todos estos detalles deben crearse o recopilarse en el servidor de Microsoft para poder realizar la configuración en FMC. Los valores principales son:

- Nombre de dominio:

Este es el nombre de dominio del servidor. En esta guía de configuración, example.com es el nombre de dominio.

- Dirección IP/FQDN del servidor:

La dirección IP o FQDN utilizado para alcanzar el servidor de Microsoft. Si se utiliza un FQDN, se debe configurar un servidor DNS en FMC y FTD para resolver el FQDN.

En esta guía de configuración, este valor es win2016.example.com (que resuelve 192.168.1.1).

- Puerto del servidor:

El puerto utilizado por el servicio LDAP. De forma predeterminada, LDAP y STARTTLS utilizan el puerto TCP 389 para LDAP, y LDAP sobre SSL (LDAPS) utiliza el puerto TCP 636.

- CA raíz:

Si se utiliza LDAPS o STARTTLS, se requiere la CA raíz utilizada para firmar el certificado SSL utilizado por LDAPS.

- Nombre de usuario y contraseña del directorio:

Se trata de la cuenta que utilizan FMC y FTD para enlazar con el servidor LDAP y autenticar usuarios y buscar usuarios y grupos.

Para ello se crea una cuenta denominada FTD Admin.

- Nombre distinguido (DN) de base y grupo:

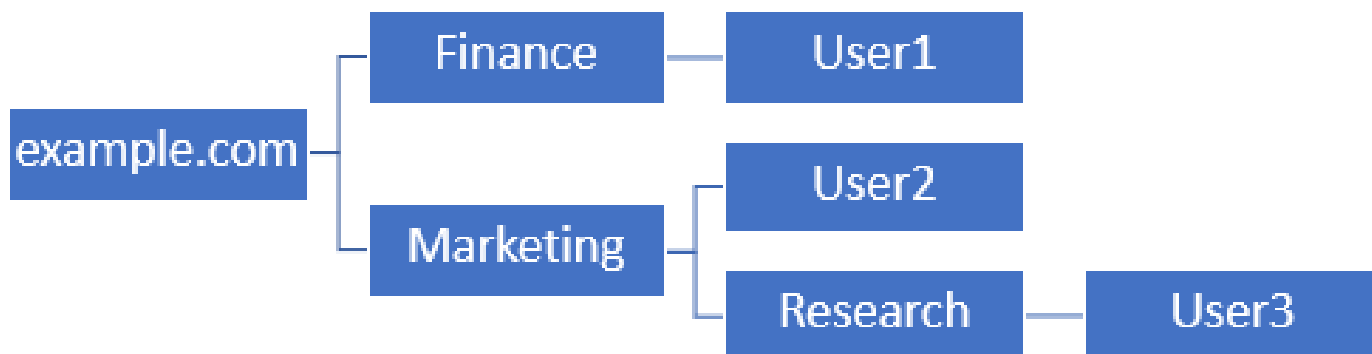
El DN base es el FMC de punto de partida y el FTD indica a Active Directory que inicie la búsqueda y autenticación de usuarios.

Del mismo modo, el DN de grupo es el punto de partida. FMC indica a Active Directory dónde debe comenzar la búsqueda de grupos para la identidad del usuario.

En esta guía de configuración, el dominio raíz `example.com` se utiliza como DN base y DN de grupo.

Sin embargo, para un entorno de producción, utilizar un DN base y un DN de grupo dentro de la jerarquía LDAP es mejor.

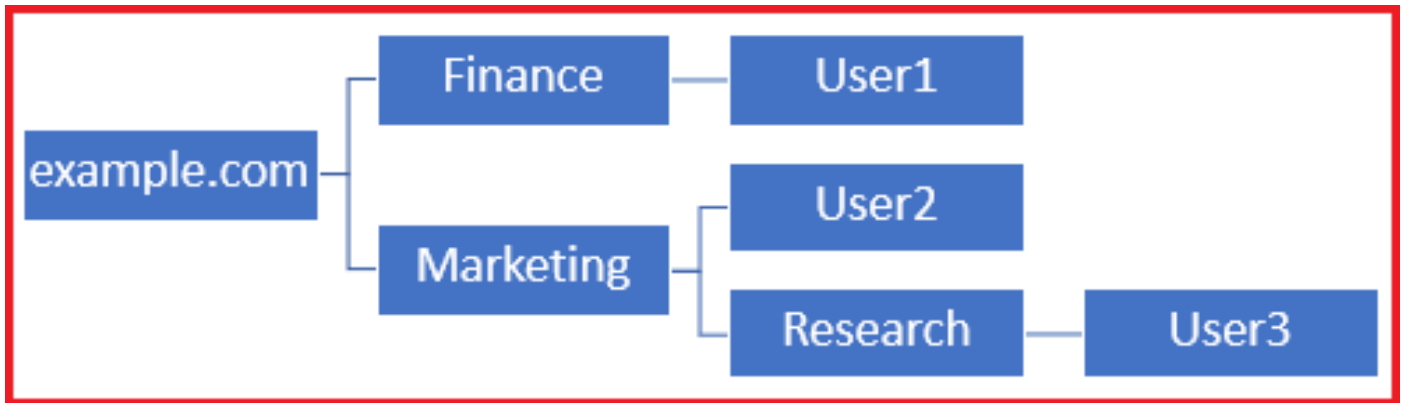
Por ejemplo, esta jerarquía LDAP:



Si un administrador desea que los usuarios de la unidad organizativa Marketing puedan autenticar el DN base, se puede establecer en la raíz (`example.com`).

Sin embargo, esto también permite que el usuario 1 de la unidad organizativa Finance inicie sesión, ya que la búsqueda de usuarios comienza en la raíz y desciende hasta Finance, Marketing e Research.

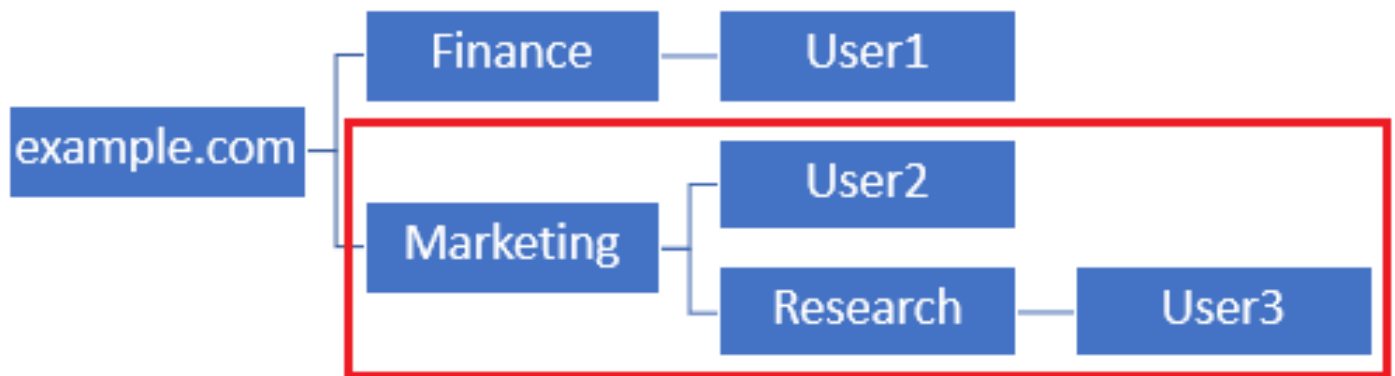
DN base establecido en `example.com`



Para restringir el inicio de sesión al único usuario de la unidad organizativa Marketing y a continuación, el administrador puede establecer el DN base en Marketing.

Ahora solo el Usuario 2 y el Usuario 3 pueden autenticarse porque la búsqueda comienza en Marketing.

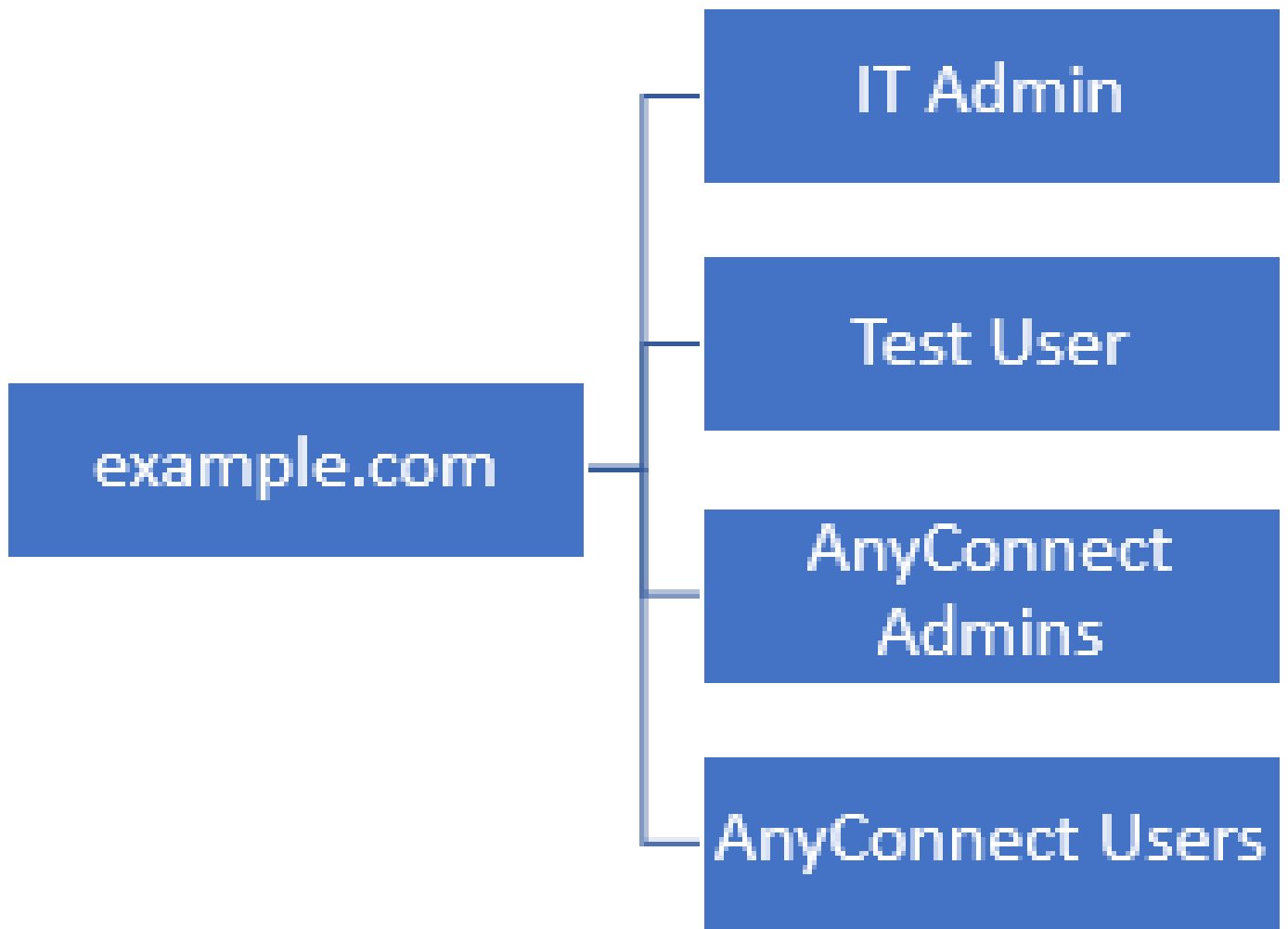
DN base establecido en Marketing



Tenga en cuenta que para un control más granular dentro del FTD para el que los usuarios pueden conectarse o asignar a los usuarios una autorización diferente en función de sus atributos AD, se debe configurar un mapa de autorización LDAP.

Puede encontrar más información al respecto aquí: [Configuración de la asignación LDAP de AnyConnect en Firepower Threat Defence \(FTD\)](#).

Esta jerarquía LDAP simplificada se utiliza en esta guía de configuración y el DN para la raíz example.com se utiliza tanto para el DN base como para el DN de grupo.



Determinar DN Base LDAP y DN de Grupo

1. Abra Usuarios y equipos de Active Directory.



Best match



Active Directory Users and Computers

Desktop app

Settings



Edit local users and groups



Change User Account Control settings



User Accounts

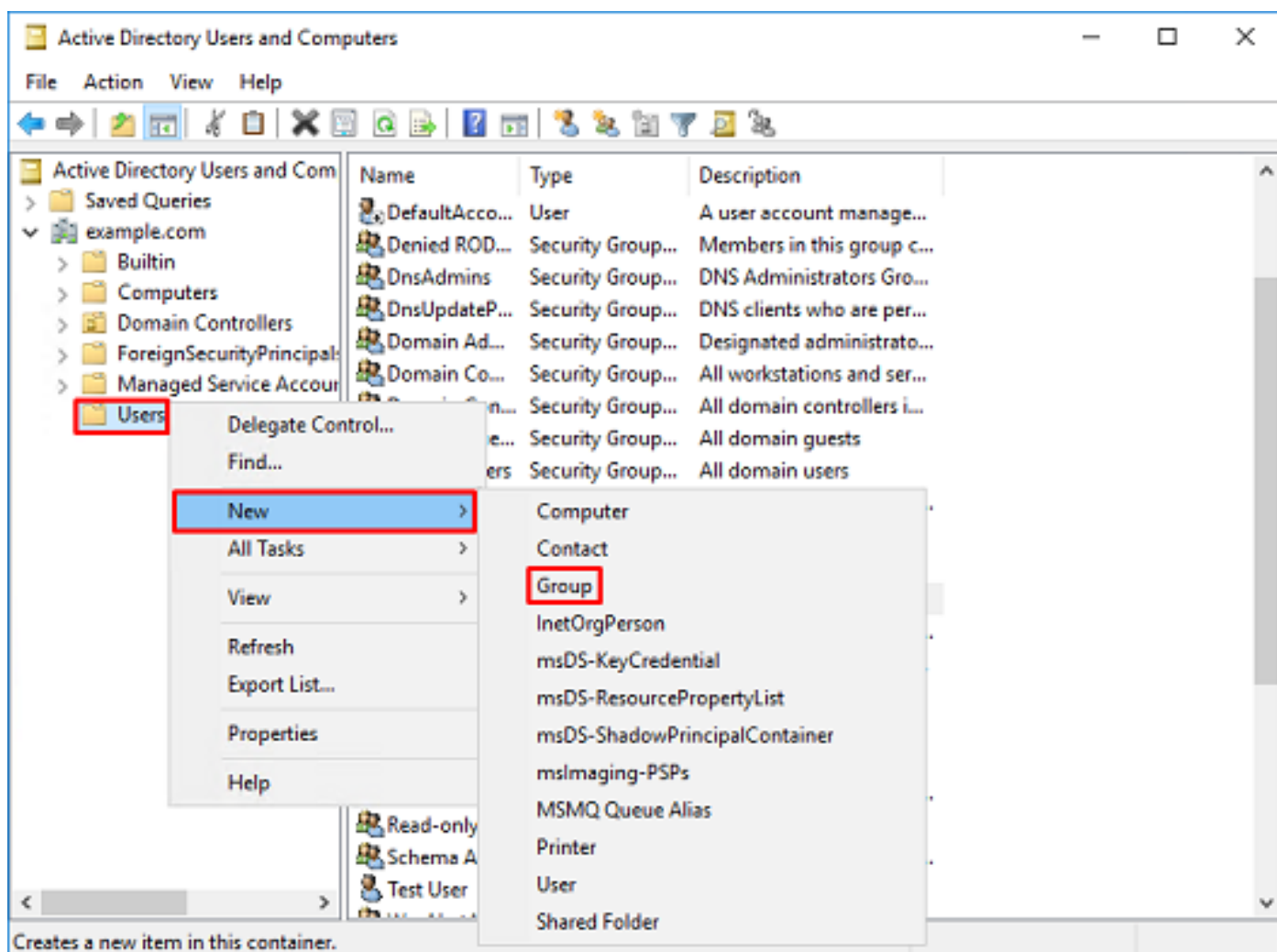


Select users who can use remote desktop




, haga clic con el botón secundario en el contenedor o unidad organizativa al que se agrega el nuevo grupo.

En este ejemplo, el grupo AnyConnect Admins se agrega bajo el contenedor Users. Haga clic con el botón derecho en Users y navegue hasta New > Group.



2. Vaya al asistente Nuevo objeto - Grupo.

New Object - Group X

 Create in: example.com/Users

Group name:

Group name (pre-Windows 2000):

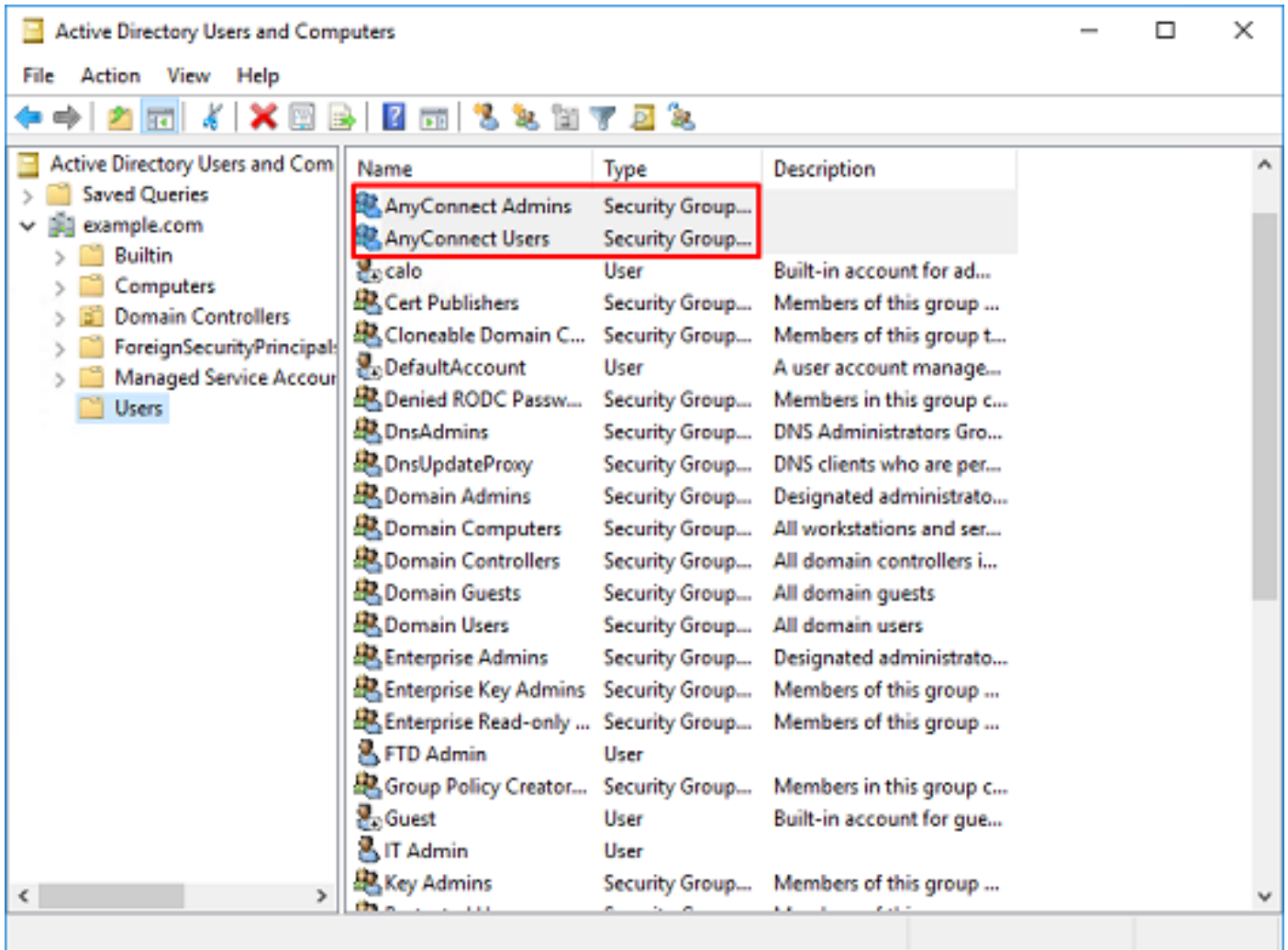
Group scope

Domain local
 Global
 Universal

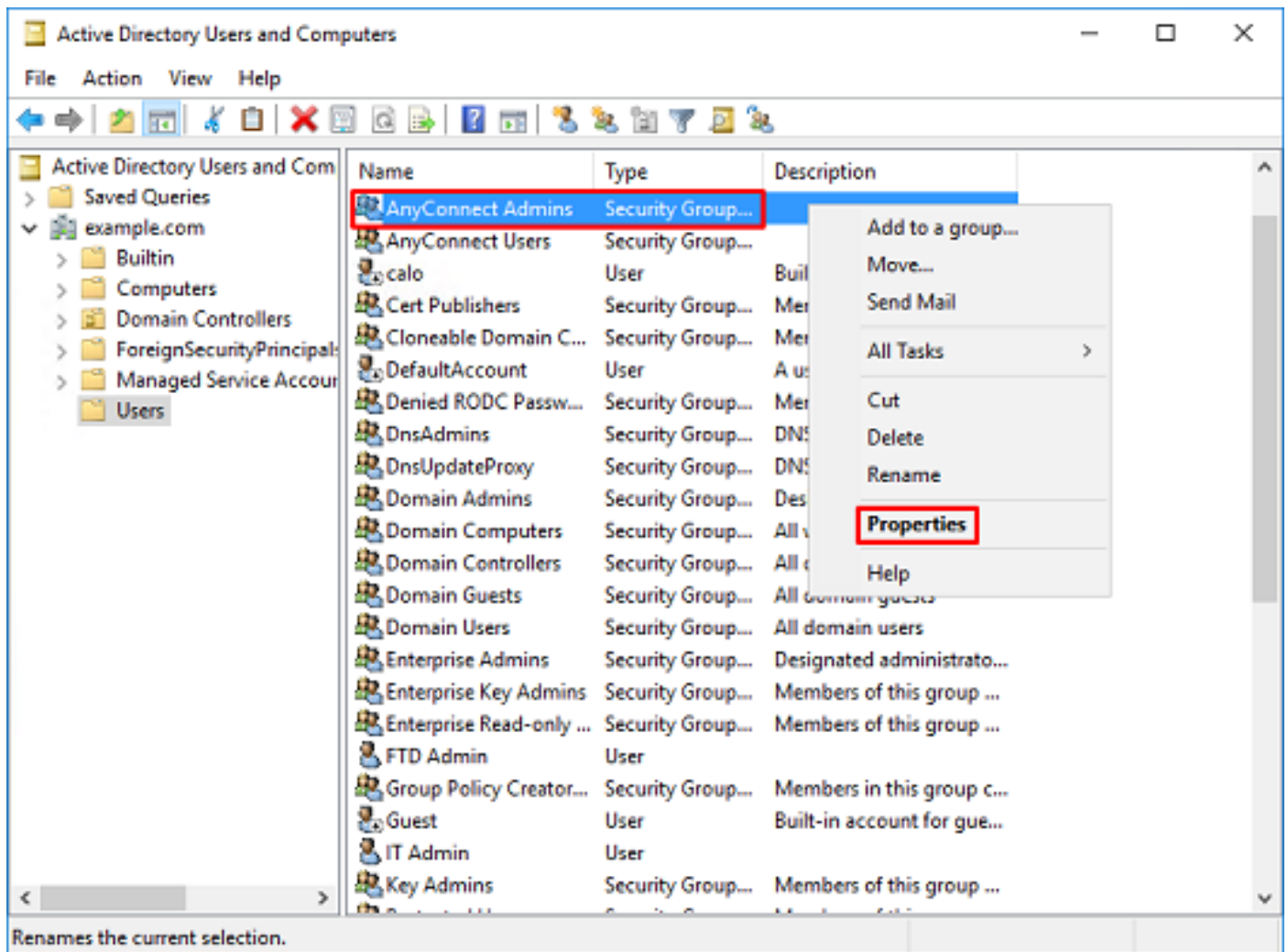
Group type

Security
 Distribution

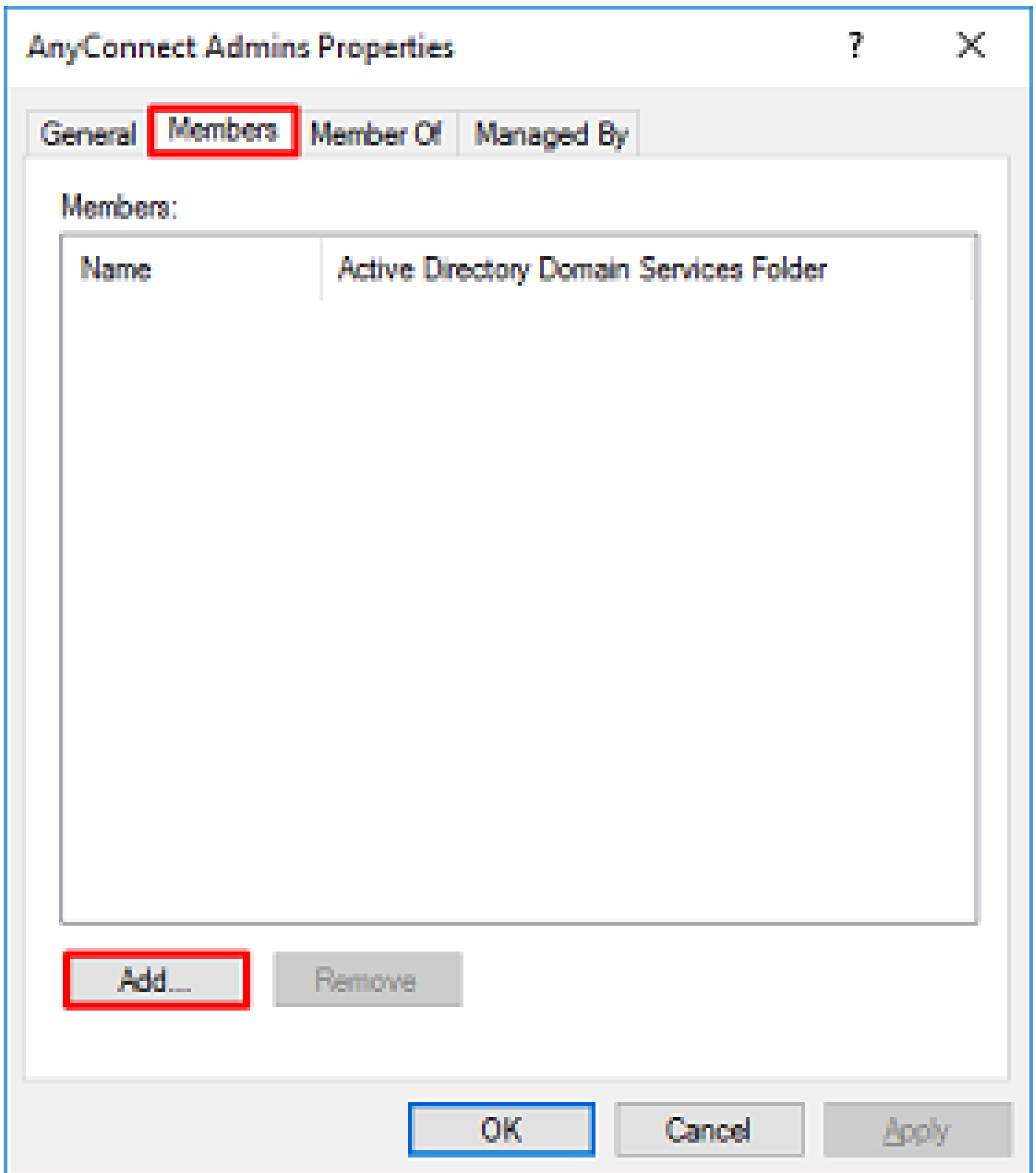
3. Compruebe que se ha creado el grupo. También se crea el grupo Usuarios de AnyConnect.



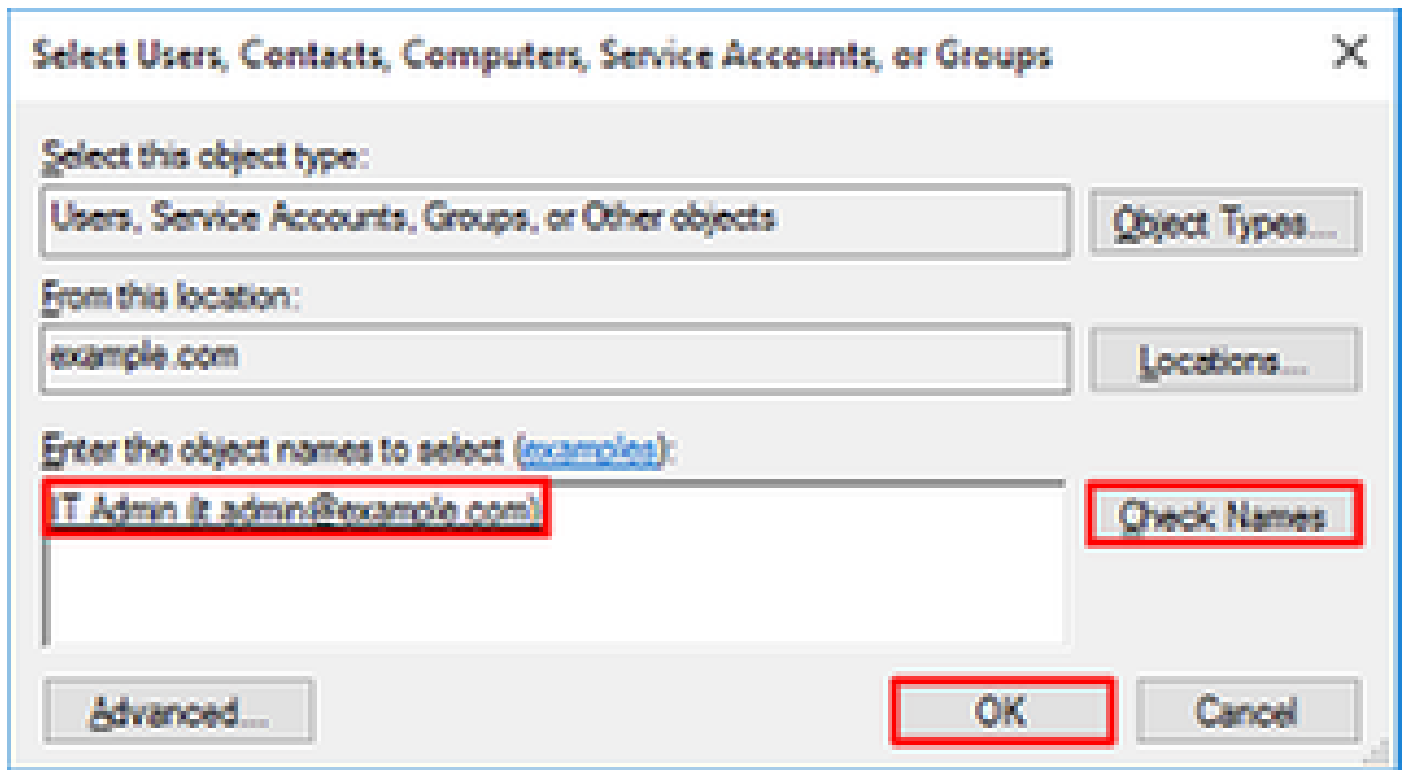
4. Haga clic con el botón derecho del ratón en el grupo de los usuarios y, a continuación, seleccione Propiedades. En esta configuración, el usuario IT Admin se agrega al grupo AnyConnect Admins y el usuario Test User se agrega al grupo AnyConnect Users.



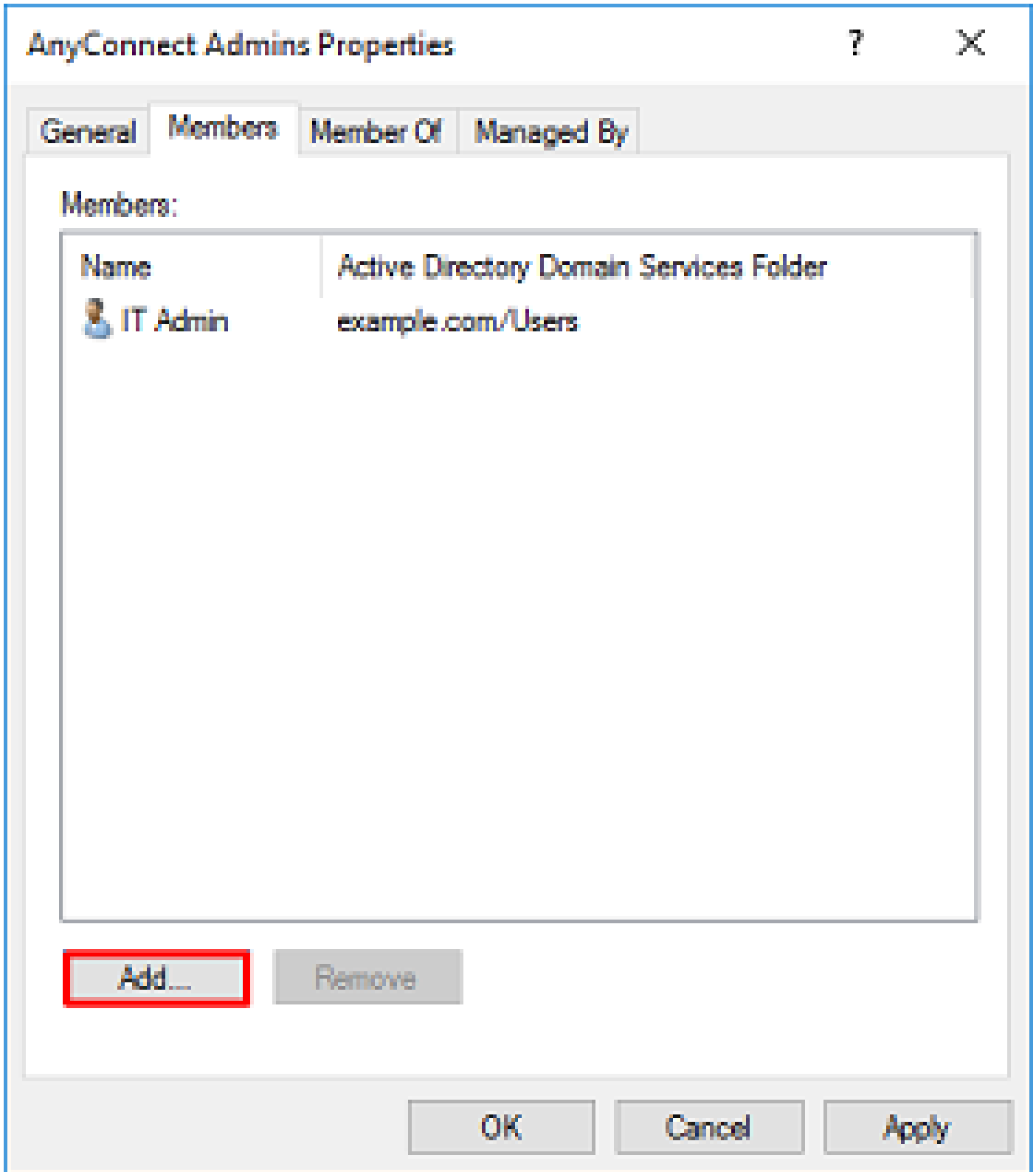
5. En la pestaña Miembros, haga clic en Agregar.



Introduzca el usuario en el campo y haga clic en Comprobar nombres para comprobar que se ha encontrado el usuario. Una vez verificado, haga clic en Aceptar.

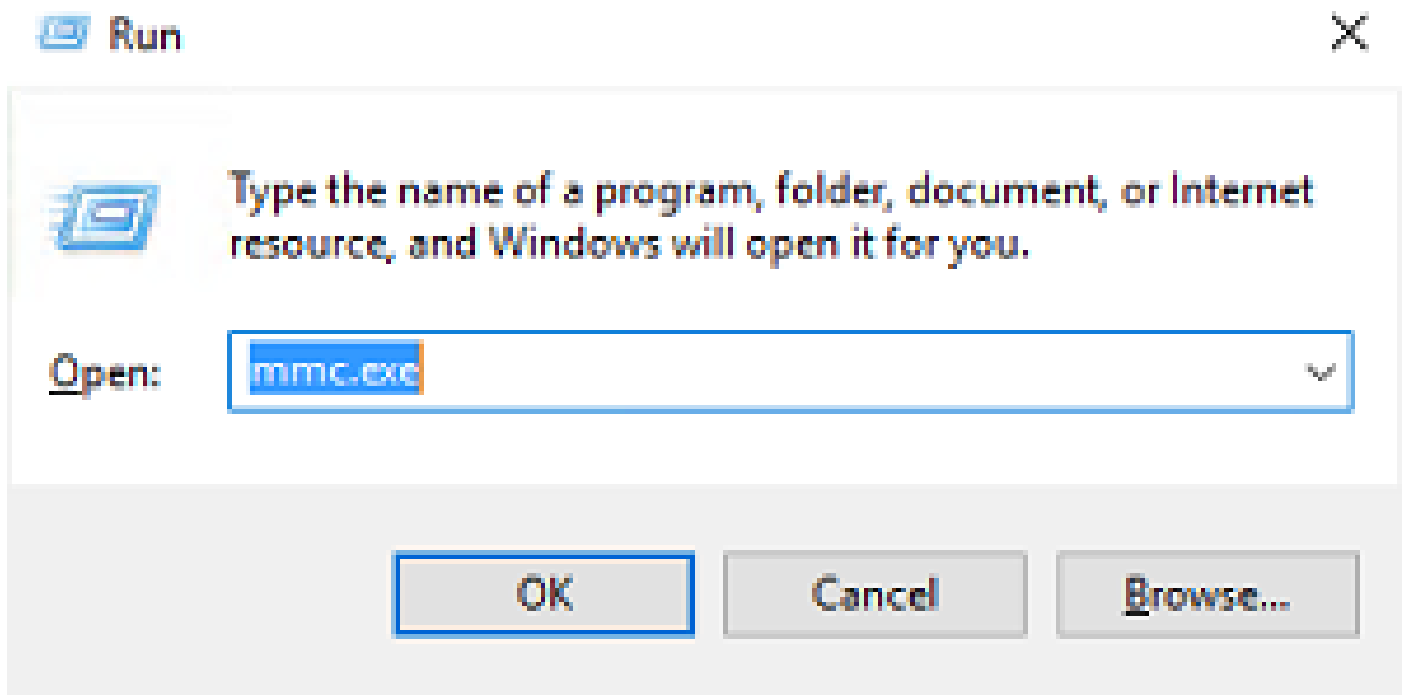


Compruebe que se ha agregado el usuario correcto y haga clic en Aceptar. El usuario Test User también se agrega al grupo AnyConnect Users siguiendo los mismos pasos.

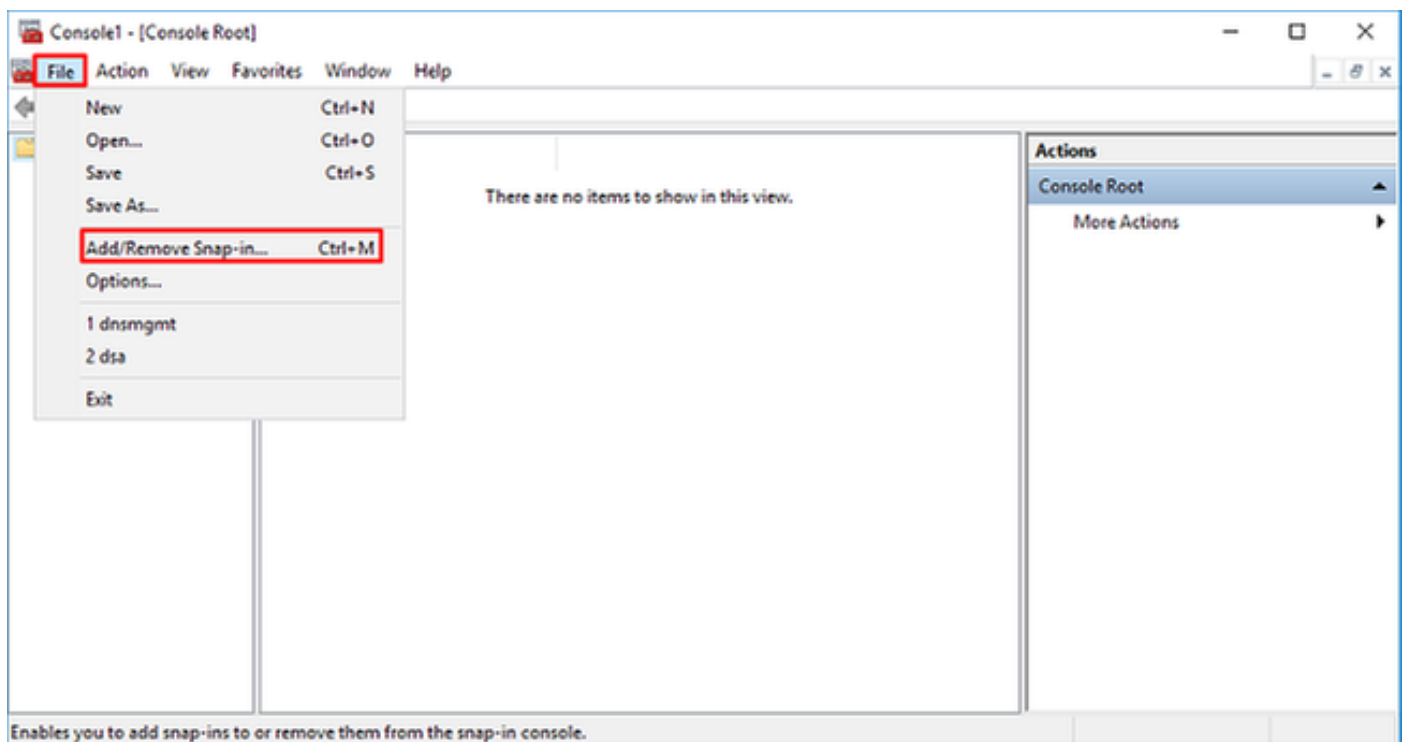


Copiar la raíz del certificado SSL LDAPS (solo se requiere para LDAPS o STARTTLS)

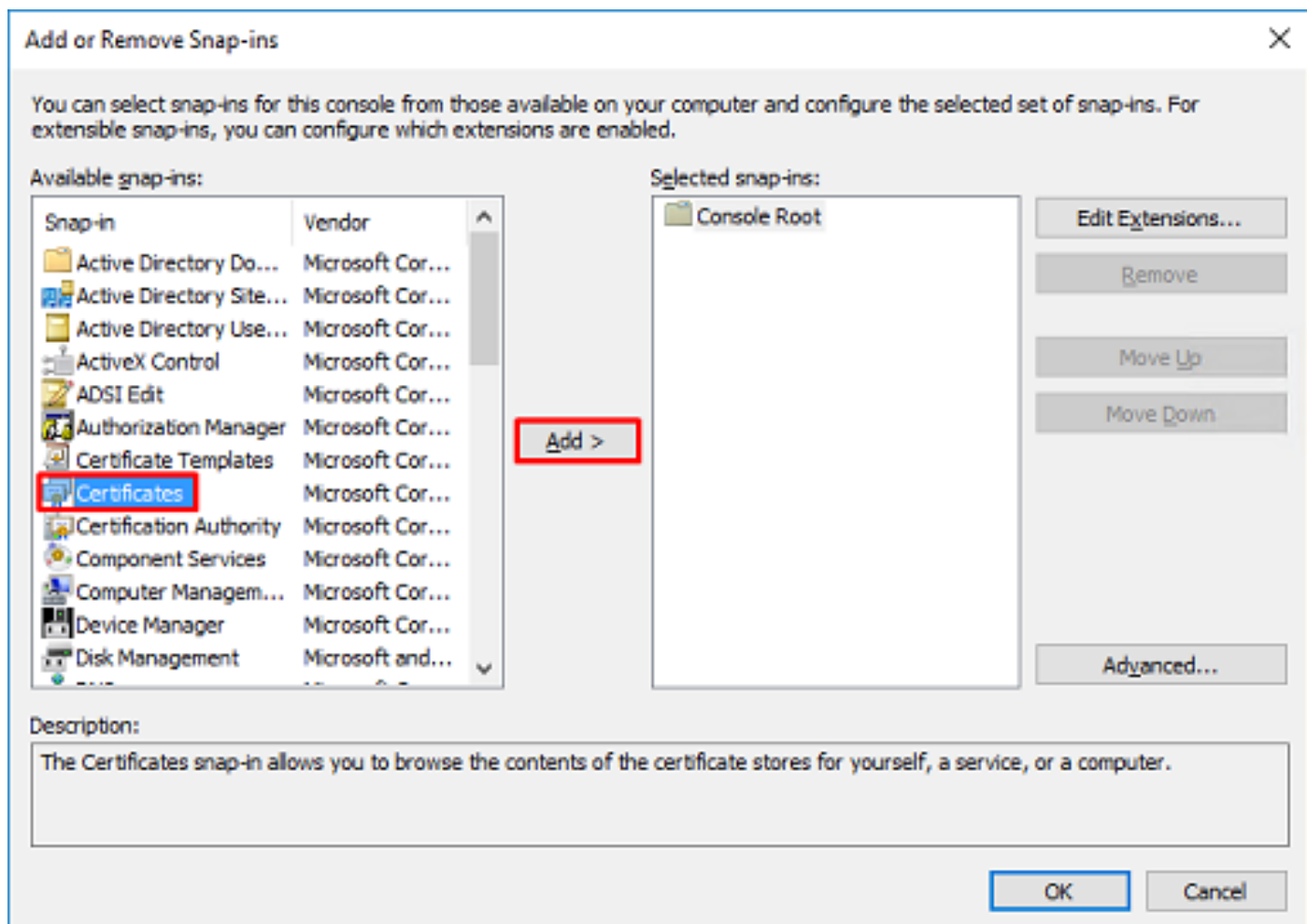
1. Presione Win+R e ingrese mmc.exe. Luego haga clic en OK (Aceptar).



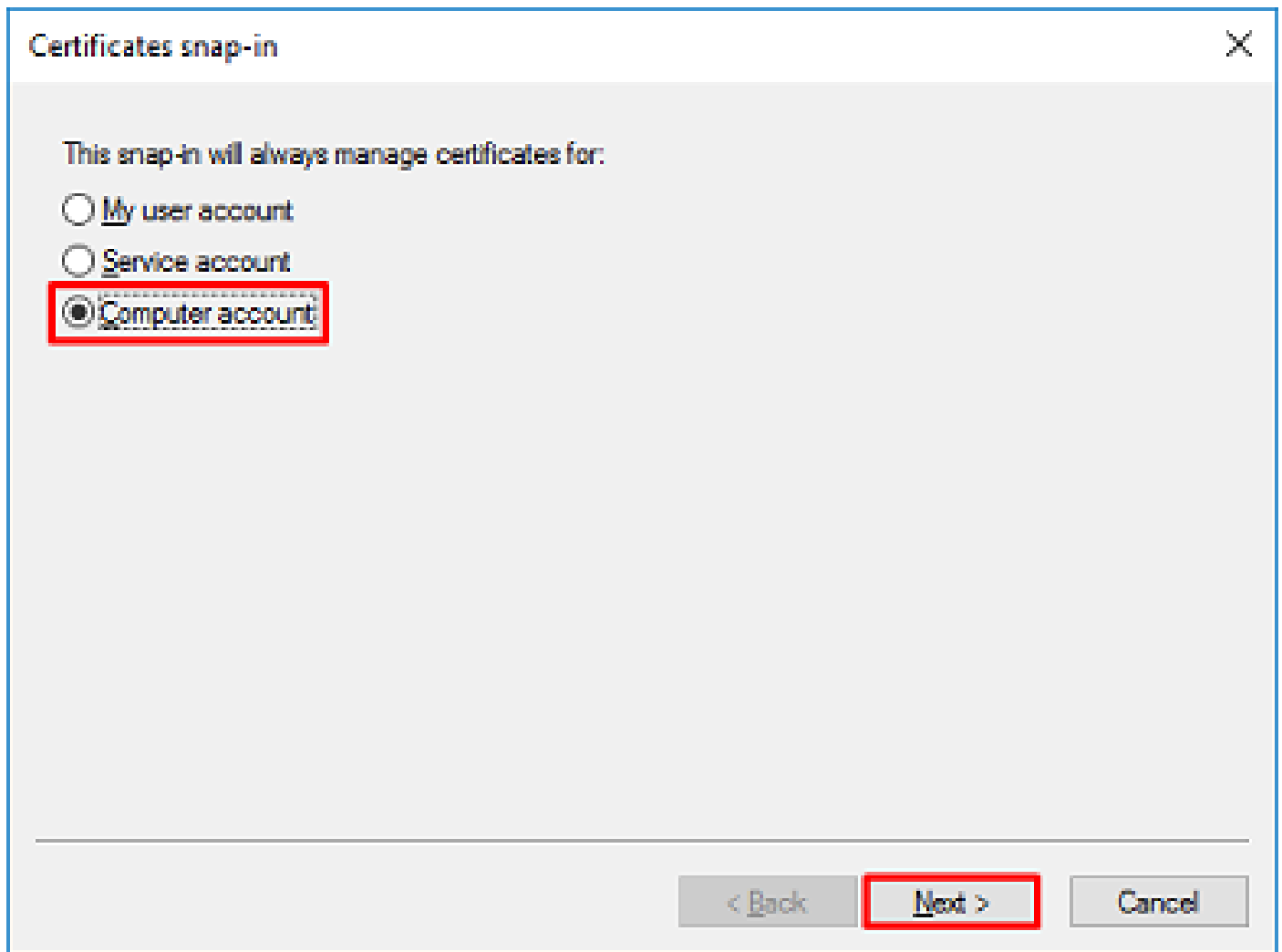
2. Vaya a Archivo > Agregar o quitar complemento.



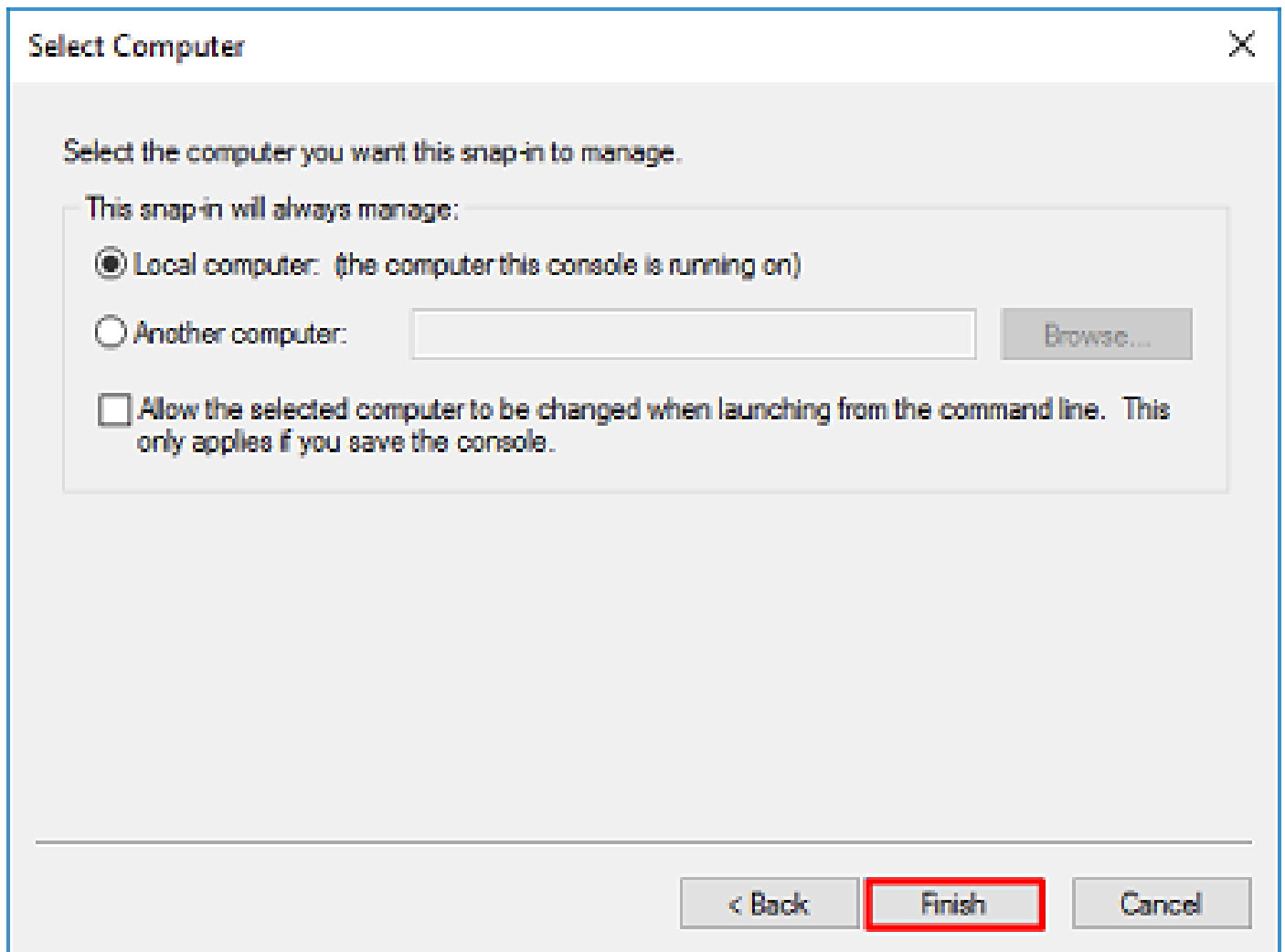
3. En Complementos disponibles, seleccione Certificados y haga clic en Agregar.



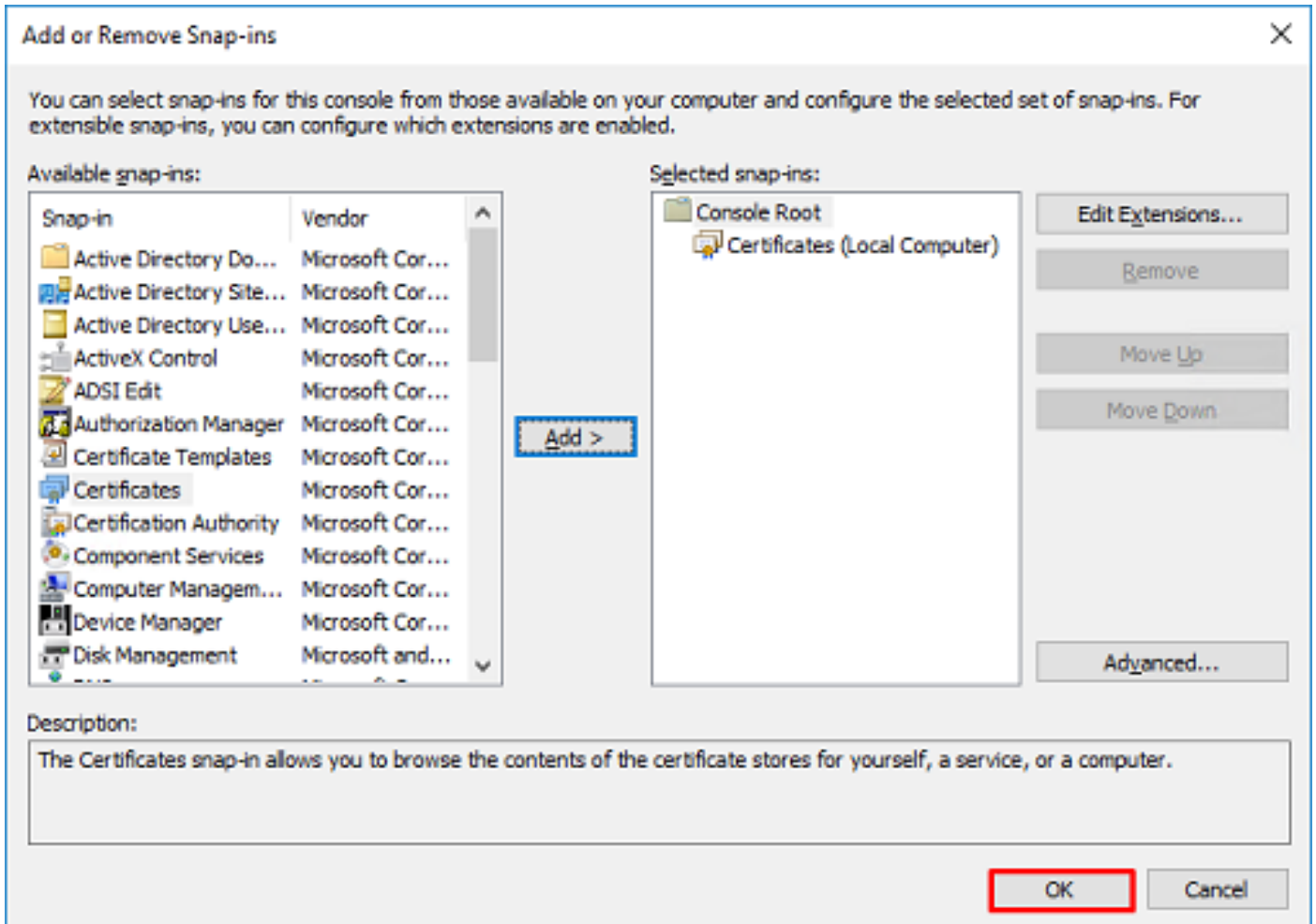
4. Seleccione Cuenta de computadora y haga clic en Siguiente.



Haga clic en Finish (Finalizar).



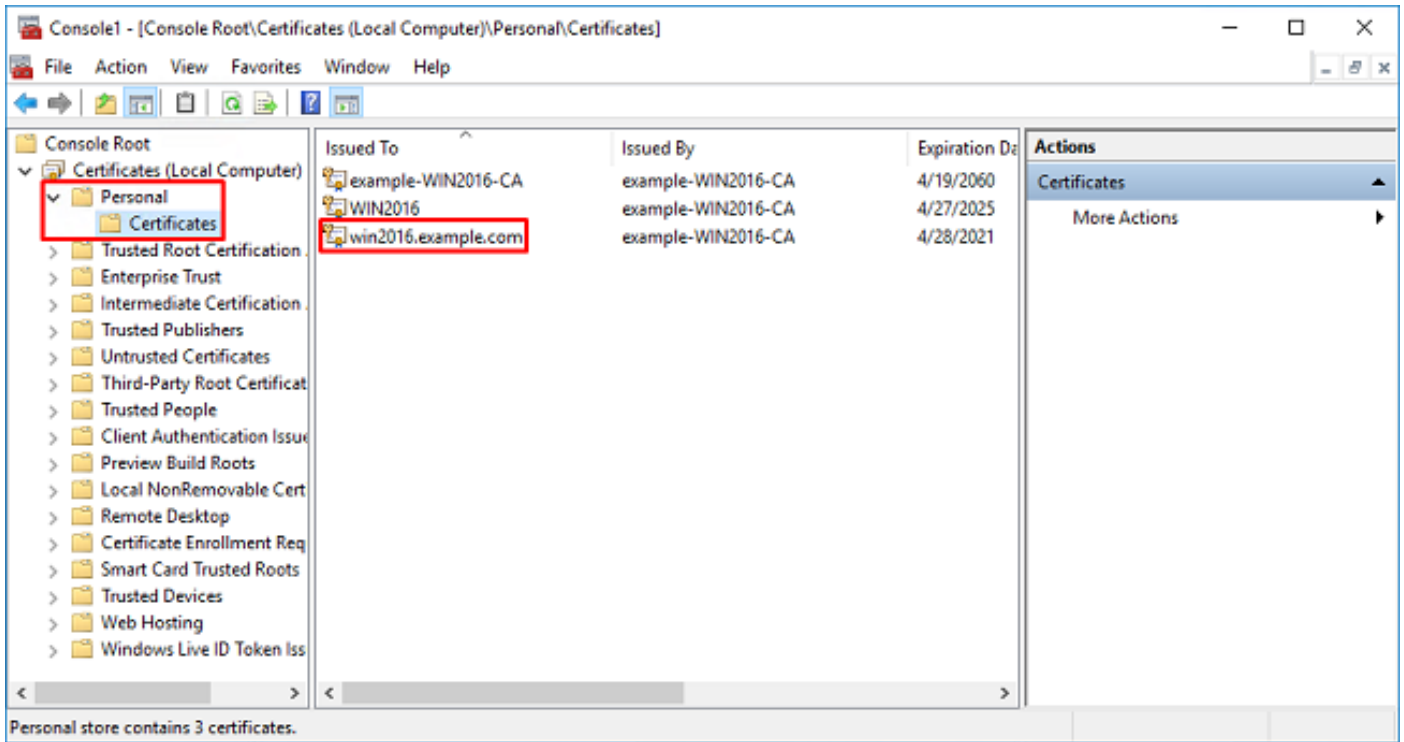
5. Haga clic en Aceptar.



6. Expanda la carpeta Personal y, a continuación, haga clic en Certificados. El certificado utilizado por LDAPS se emite para el nombre de dominio completo (FQDN) del servidor de Windows. En este servidor, hay 3 certificados listados.

- Un certificado de CA emitido a y por ejemplo-WIN2016-CA.
- Certificado de identidad emitido para WIN2016 por example-WIN2016-CA.
- Certificado de identidad emitido para win2016.example.com por example-WIN2016-CA.

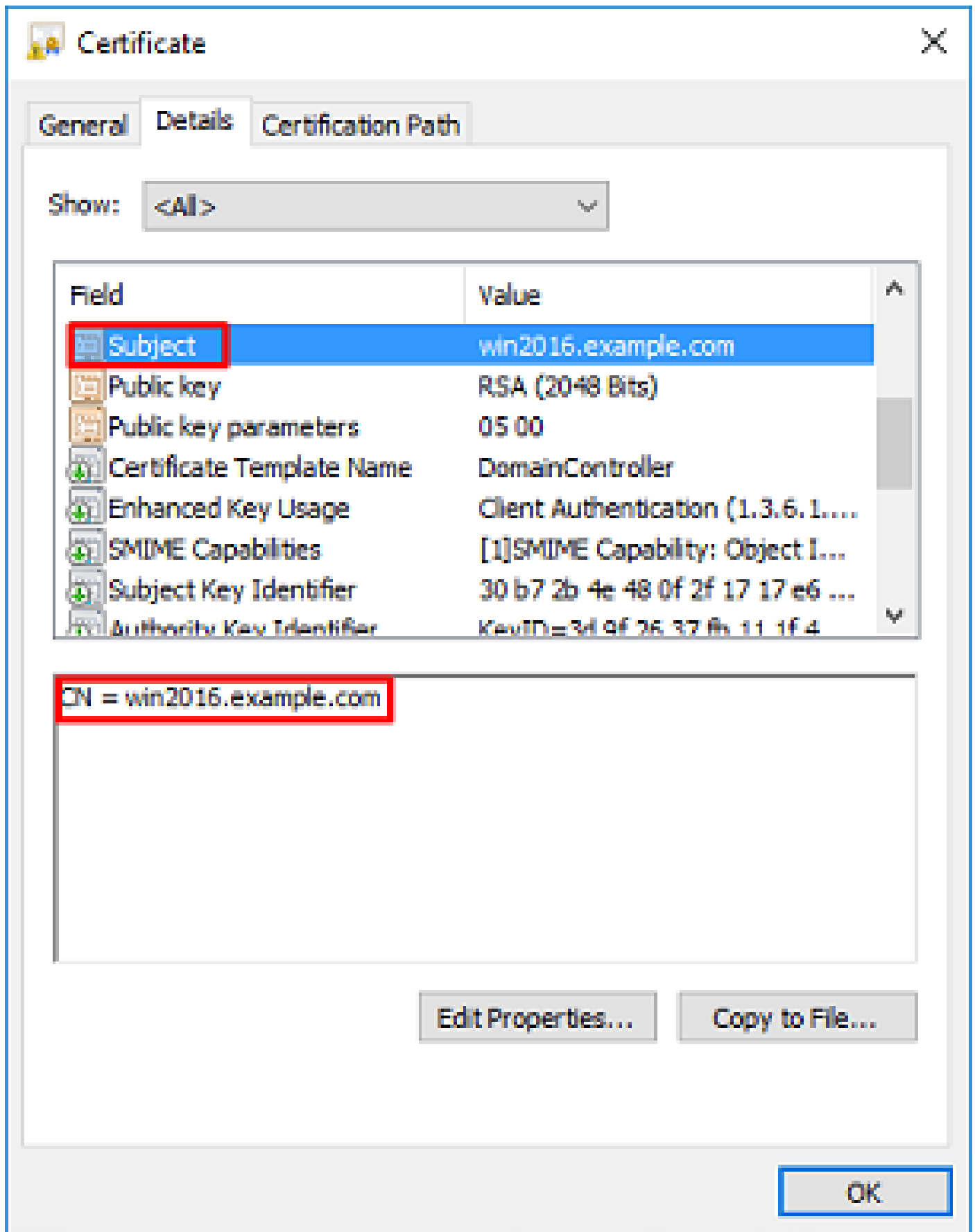
En esta guía de configuración, el FQDN es win2016.example.com y, por lo tanto, los 2 primeros certificados no son válidos para su uso como certificado SSL LDAP. El certificado de identidad emitido para win2016.example.com es un certificado emitido automáticamente por el servicio de CA de Windows Server. Haga doble clic en el certificado para comprobar los detalles.



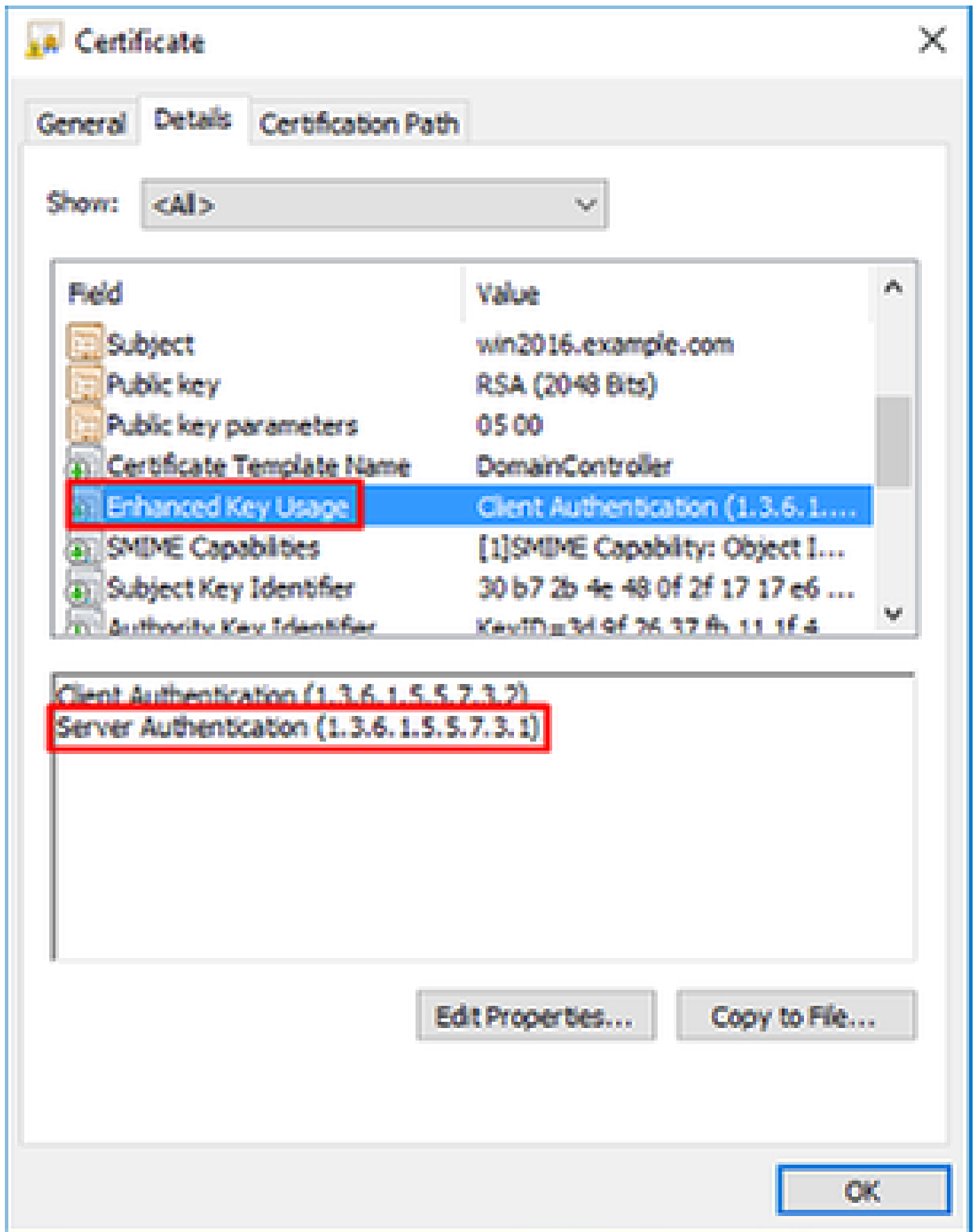
7. Para ser utilizado como certificado SSL LDAPS, el certificado debe cumplir estos requisitos:

- El nombre común o el nombre alternativo de sujeto DNS coincide con el FQDN del servidor de Windows.
- El certificado tiene Autenticación del servidor en el campo Uso mejorado de clave.

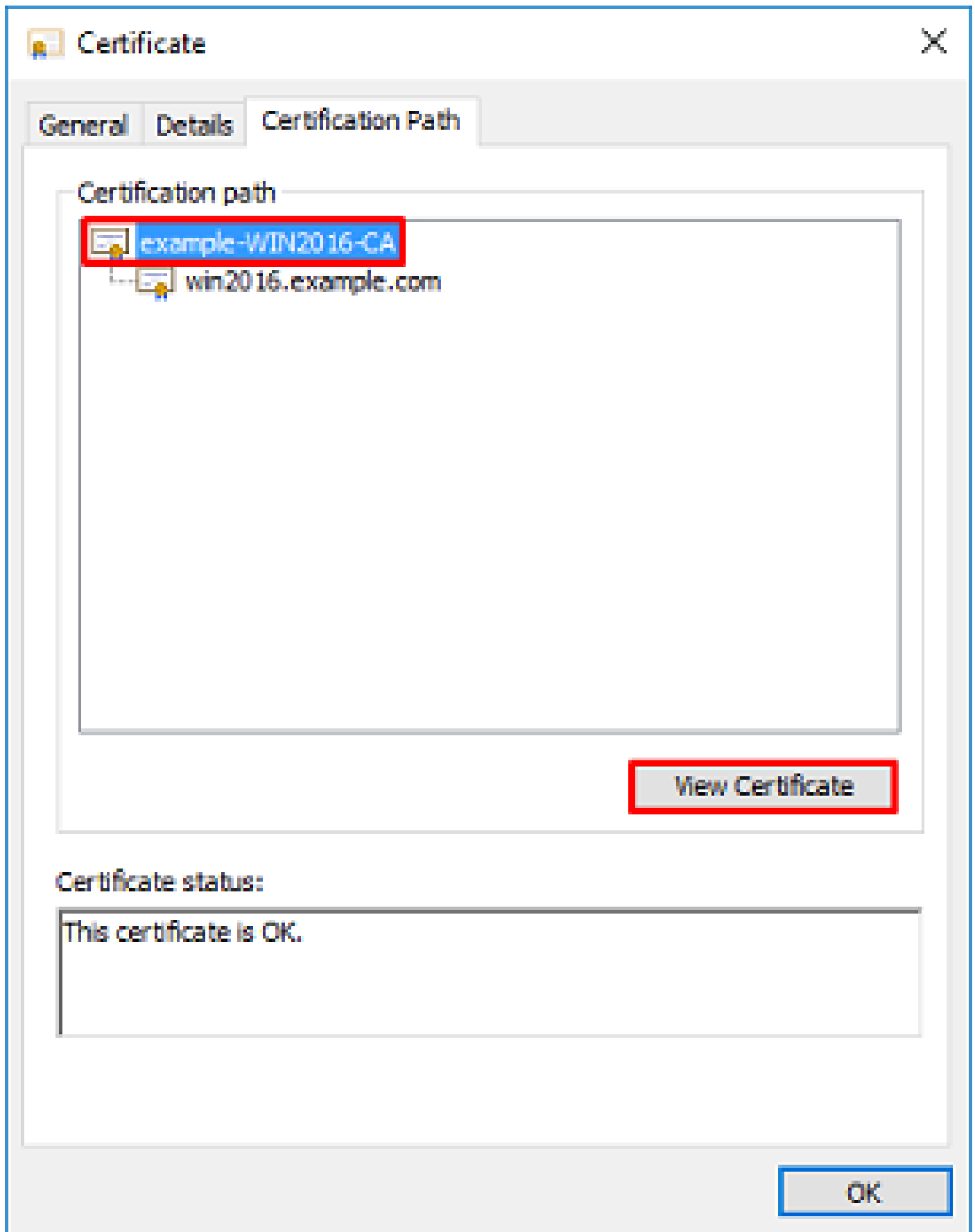
En la pestaña Detalles del certificado, seleccione Asunto y Nombre alternativo del sujeto, el FQDN win2016.example.com está presente.



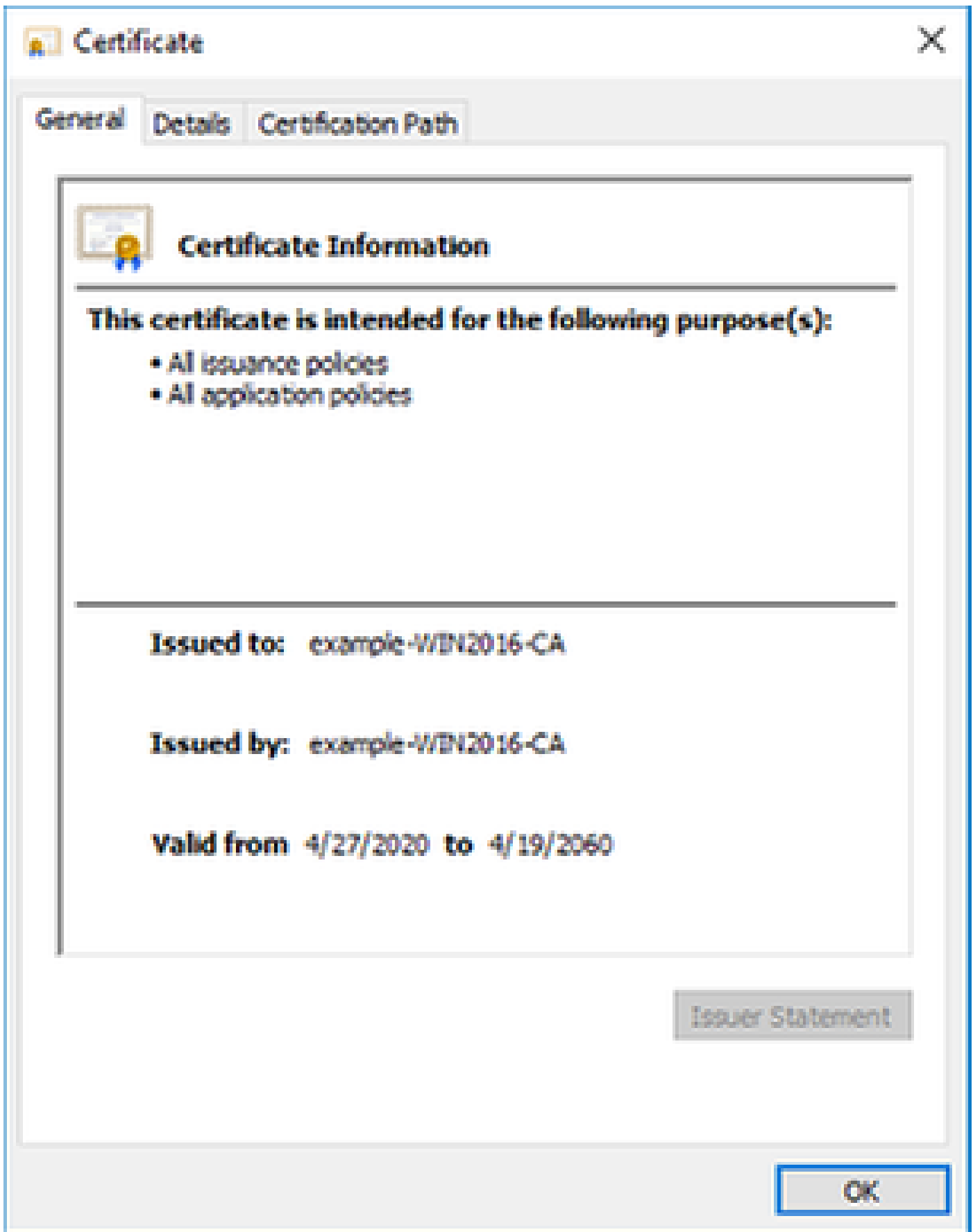
En Enhanced Key Usage, Server Authentication está presente.



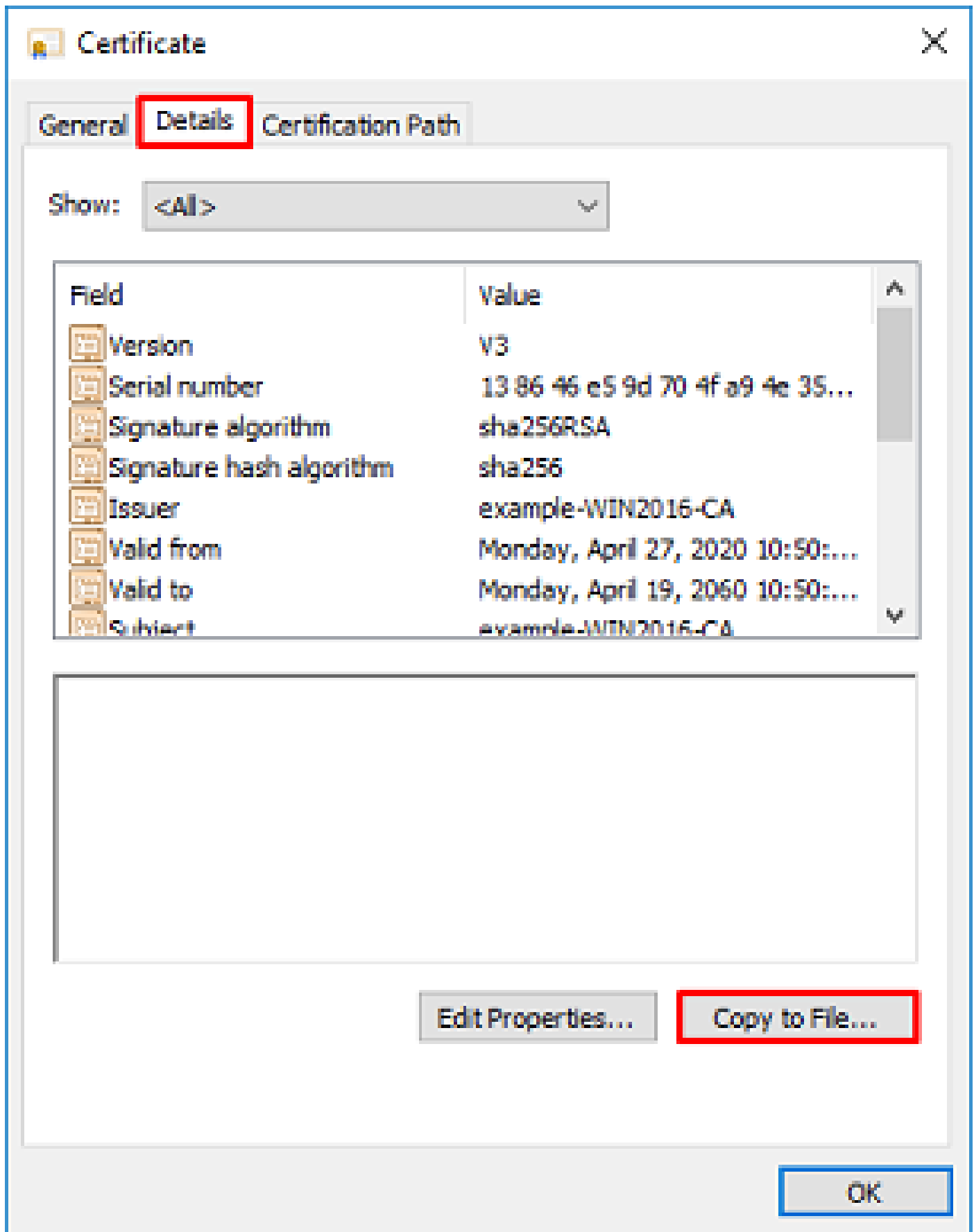
8. Una vez confirmado, en la pestaña Ruta de certificación, seleccione el certificado superior que es el certificado de CA raíz y, a continuación, haga clic en Ver certificado.



9. Se abrirán los detalles de Certificados para el certificado de CA raíz.



En la pestaña Details, haga clic en Copy to File.



10. Vaya al Asistente para exportación de certificados. El asistente exporta la CA raíz en formato PEM.



←  Certificate Export Wizard

Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

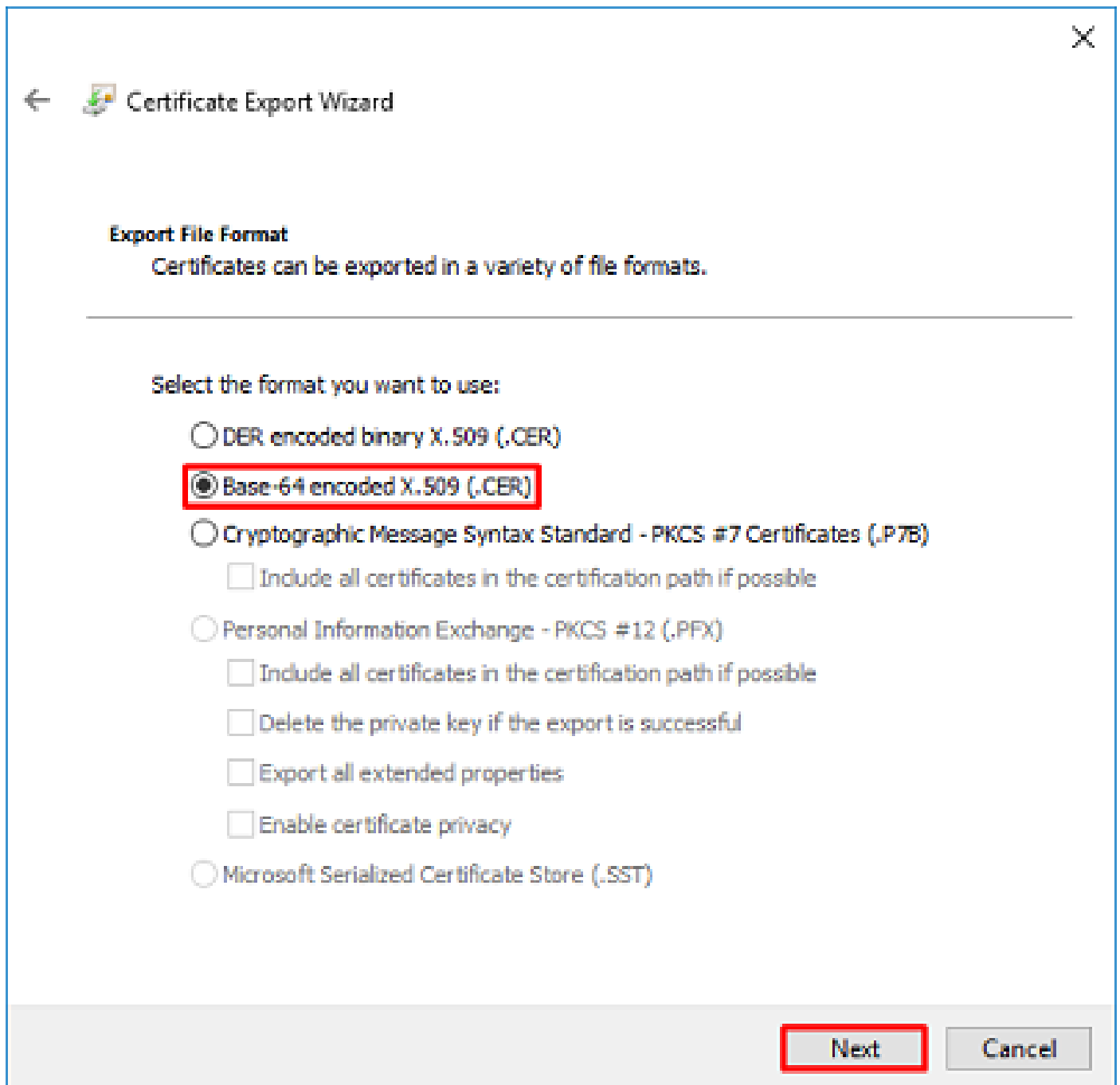
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Next

Cancel

Seleccione Base-64 codificado X.509.



Seleccione el nombre del archivo y a dónde se exporta.



←  Certificate Export Wizard

File to Export

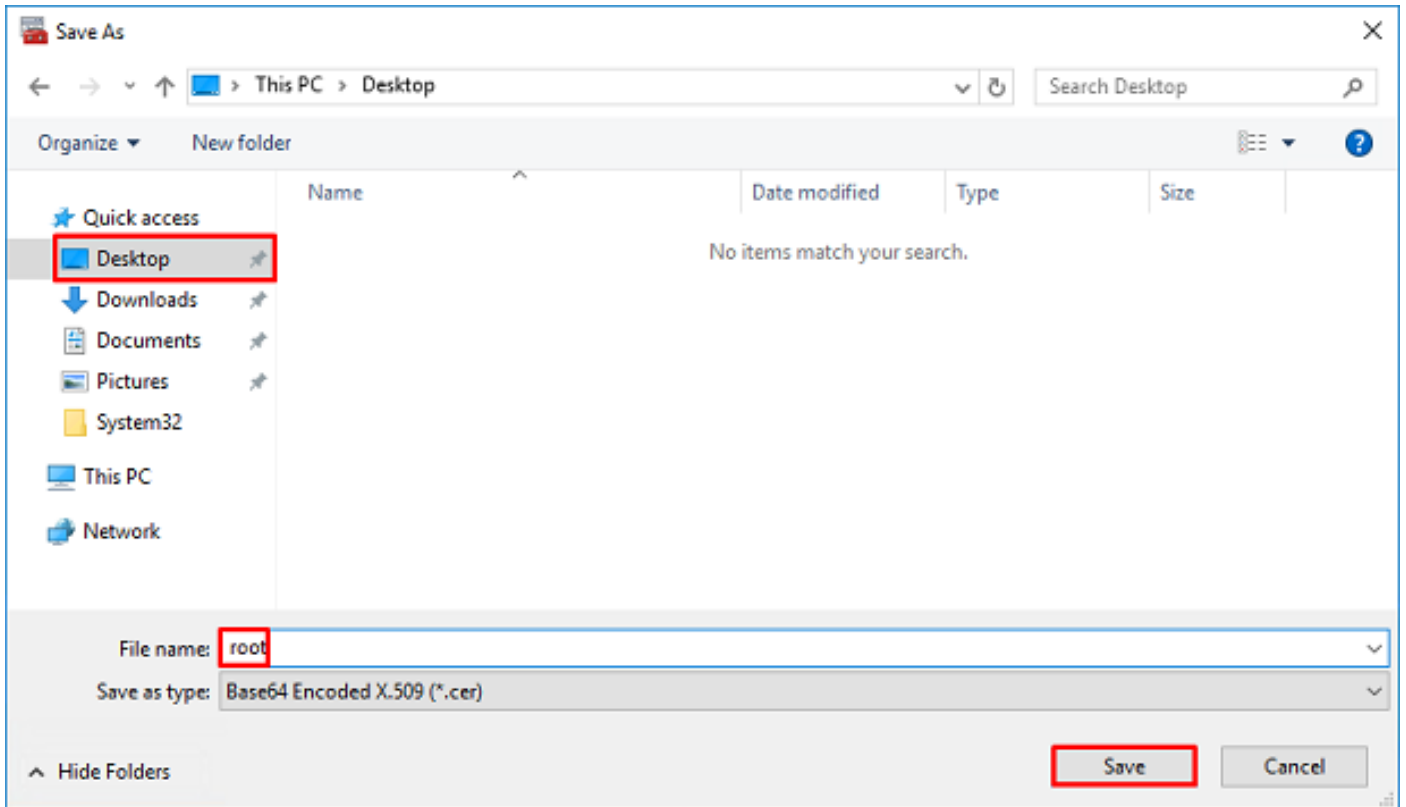
Specify the name of the file you want to export

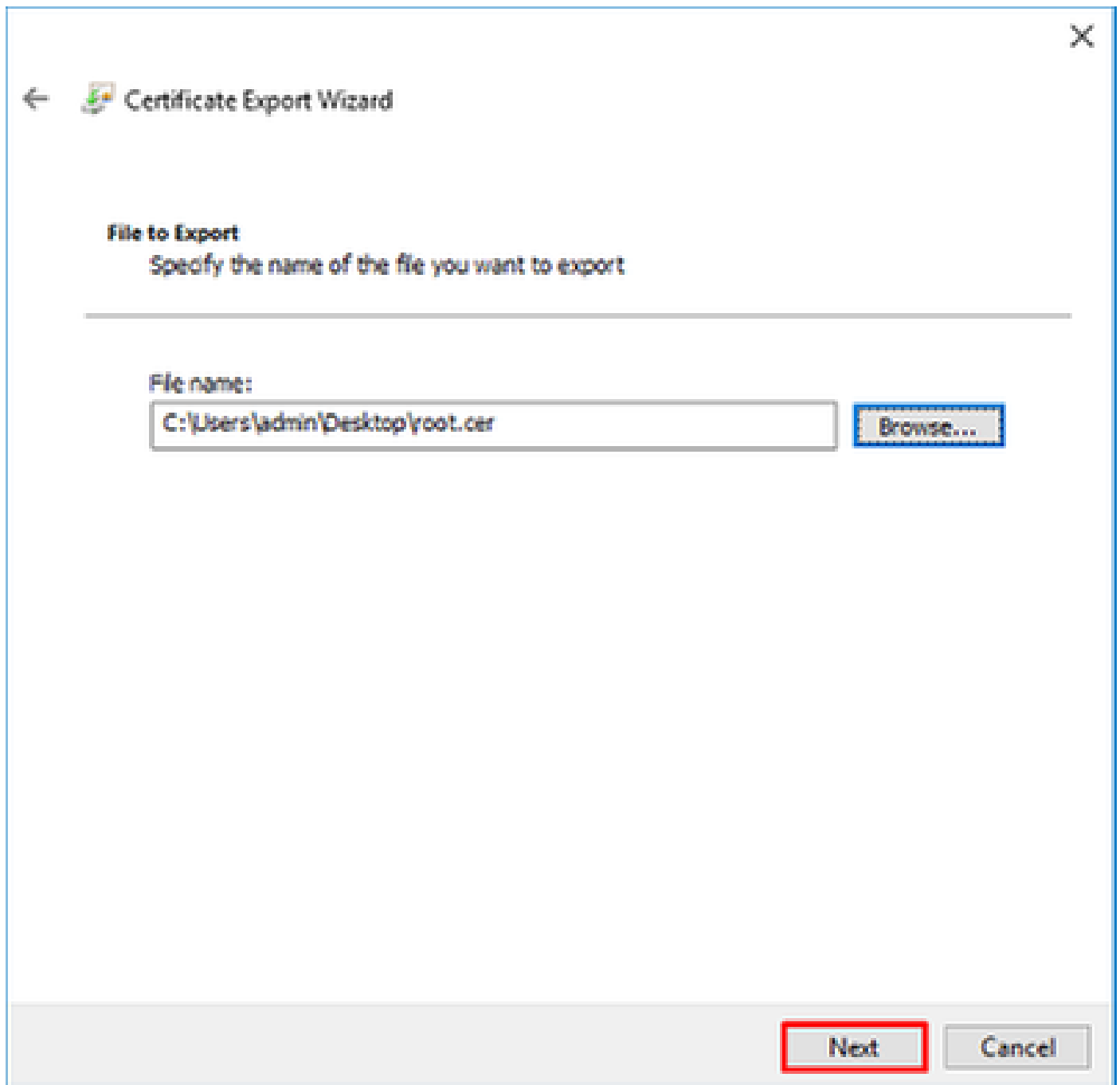
File name:

Browse...

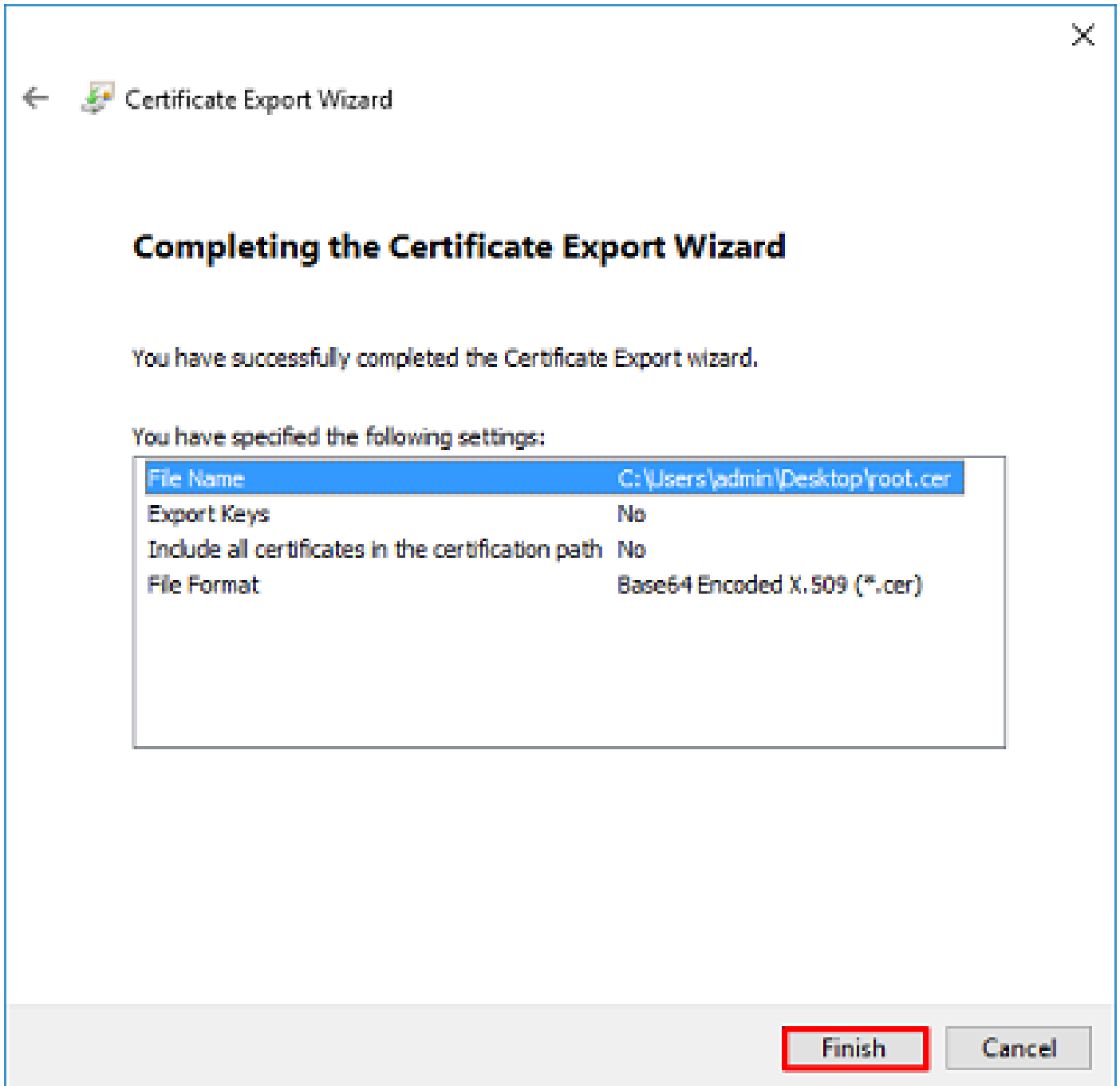
Next

Cancel





Ahora haga clic en Finish.



11. Desplácese hasta la ubicación y abra el certificado con un bloc de notas u otro editor de texto. Muestra el certificado de formato PEM. Guarde esto para más tarde.

```
-----BEGIN CERTIFICATE-----  
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT61ONTjooEQyMTANBgkqhkiG9w0BAQsFADAd  
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP  
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YV1wbGUtV010MjAxNi1DQTCC  
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b  
Ya+PngsxMyvkewP33QLTAww1HW1Tb9Mk5BDW0ItTaVsgHwPbf+++++m+bln3AiZnHV  
00+k6dVVY/E5qVkeKSGoY+v940S23161zdwReMOFhgbc2qMertIoficrRihonuU  
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfa1LPuM  
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/  
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPfkMA3u8C  
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O  
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
```

```
vzwVD3c5Q1nrNP+6Mq620FpYH91k4Ch9S5g/CEOemhcgw8MDIoxW2dTsjenAEt7r  
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmT0vdNVib7Xp11IVa  
6tALTt3ANRNgREtXPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscubR1+D  
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/y1cdwNSJFfQV3DgZg+R96  
9WLCR30big6xyo9Zu+1ixcWpdrbAD06zMhbEYEhkh00jBrUEBBI6Cy83iTZ9ejsk  
KgwBJXEu33Pp1W6E  
-----END CERTIFICATE-----
```

12. (Opcional) En el caso de que haya múltiples certificados de identidad que puedan ser utilizados por LDAPS y haya incertidumbre sobre cuál se utiliza, o no haya acceso al servidor LDAPS, es posible extraer la ca raíz de una captura de paquetes realizada en el servidor Windows o FTD después.

Configuraciones de FMC

Verificar licencia

Para implementar la configuración de AnyConnect, el FTD debe estar registrado con el servidor de licencias inteligentes, y se debe aplicar al dispositivo una licencia válida Plus, Apex o VPN Only.

1. Vaya a System > Licenses > Smart Licensing.



2. Compruebe que los dispositivos cumplen los requisitos y que se han registrado correctamente. Asegúrese de que el dispositivo esté registrado con una licencia AnyConnect Apex, Plus o VPN Only License.

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Smart Licenses Health Monitoring Tools

Smart License Status Cisco Smart Software Manager

Usage Authorization:	Authorized (Last Synchronized On May 03 2020)
Product Registration:	Registered (Last Renewed On Mar 03 2020)
Assigned Virtual Account:	SEC TAC
Export-Controlled Features:	Enabled
Cisco Success Network:	Disabled
Cisco Support Diagnostics:	Disabled

Smart Licenses Filter Devices... Edit Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
Firepower Management Center Virtual (2)	✓			
Base (2)	✓			
Malware (1)	✓			
Threat (2)	✓			
URL Filtering (2)	✓			
AnyConnect Apex (1)	✓			
FTD-2 192.168.1.17 - Cisco Firepower Threat Defense for VMWare - v6.3.0	✓	Cisco Firepower Threat Defense for VMWare	Global	N/A
AnyConnect Plus (0)				
AnyConnect VPN Only (0)				

Note: Container Instances of same blade share feature licenses

Rango de configuración

1. Vaya a Sistema > Integración.

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains **Integration** Updates Licenses Health Monitoring Tools

2. En Rangos, haga clic en Nuevo rango.

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains **Integration** Updates Licenses Health Monitoring Tools

Cloud Services **Realms** Identity Sources eStreamer Host Input Client Smart Software Satellite

Compare realms New realm

Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
------	-------------	--------	------	---------	----------	-----------------	-------

3. Rellene los campos correspondientes según la información recopilada del servidor de Microsoft. Luego haga clic en OK (Aceptar).

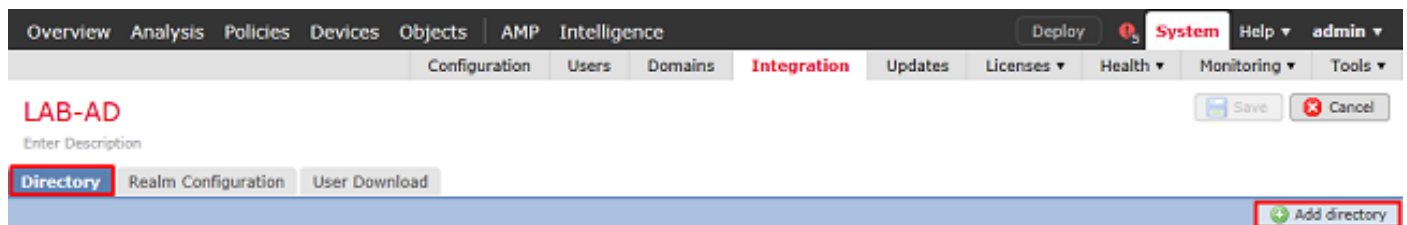
Add New Realm



Name *	<input type="text" value="LAB-AD"/>	
Description	<input type="text"/>	
Type *	<input type="text" value="AD"/>	
AD Primary Domain *	<input type="text" value="example.com"/>	ex: domain.com
AD Join Username	<input type="text"/>	ex: user@domain
AD Join Password	<input type="password"/>	<input type="button" value="Test AD Join"/>
Directory Username *	<input type="text" value="ftd.admin@example.com"/>	ex: user@domain
Directory Password *	<input type="password" value="*****"/>	
Base DN *	<input type="text" value="DC=example,DC=com"/>	ex: ou=user,dc=cisco,dc=com
Group DN *	<input type="text" value="DC=example,DC=com"/>	ex: ou=group,dc=cisco,dc=com
Group Attribute	<input type="text" value="Member"/>	

* Required Field

4. En la nueva ventana, seleccione Directorio si aún no está seleccionado, pulse Añadir directorio.



Rellene los detalles del servidor de AD. Tenga en cuenta que si se utiliza el FQDN, FMC y FTD no se podrán enlazar correctamente a menos que DNS esté configurado para resolver el FQDN.

Para configurar DNS para FMC, navegue hasta System > Configuration y seleccione Management Interfaces.

Para configurar DNS para el FTD, navegue hasta Devices > Platform Settings, cree una nueva política o edite una actual y luego vaya a DNS.

Add directory



Hostname / IP Address	<input type="text" value="win2016.example.com"/>
Port	<input type="text" value="389"/>
Encryption	<input type="radio"/> STARTTLS <input type="radio"/> LDAPS <input checked="" type="radio"/> None
SSL Certificate	<input type="text"/>

Si se utiliza LDAPS o STARTTLS, haga clic en el símbolo verde + (más), asigne un nombre al certificado y copie el certificado de CA raíz con formato PEM. A continuación, haga clic en Guardar.

Import Trusted Certificate Authority



Name:	<input type="text" value="LDAPS_ROOT"/>
Certificate Data or, choose a file:	<input type="button" value="Browse.."/>
<pre>-----BEGIN CERTIFICATE----- MIIDCCCAfCgAwIBAgIQE4ZG5Z1wt6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDEwJleGFtZXQxLlVdJTJiIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTIaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC ASIWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl8ghT719NzSQpoQPh0YT67b Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV OO+k6dVVY/E5qVKEKSGoY+v940S2316lzdwrEMOFhgbc2qMertIoficrRihonuU Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkFA1LPuM aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWIRnUIQBUaLdQaabhipD/ sVs5PneYJX8YKma821uYI6j90YuytmsHBTcIeyC062a8BKqOL7N86HFPFkMA3u8C AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O BBYEFD2fj7ER9EM/HCxVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcgw8MDIoxW2dTsjenAET7r phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa 6tALTt3ANRNgREtPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjIBCxsTscubRI+D dLEFKQqmMeYvkvf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFFQV3DgZg+R96 9WLCR30big6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk KgwBJXEu33PplW6E -----END CERTIFICATE-----</pre>	
<input type="checkbox"/> Encrypted, and the password is:	<input type="text"/>

Seleccione la CA raíz recién agregada en el menú desplegable junto a Certificado SSL y haga clic en STARTTLS o LDAPS.

Edit directory



Hostname / IP Address	<input type="text" value="win2016.example.com"/>
Port	<input type="text" value="636"/>
Encryption	<input type="radio"/> STARTTLS <input checked="" type="radio"/> LDAPS <input type="radio"/> None
SSL Certificate	<input type="text" value="LDAPS_ROOT"/>

Haga clic en Test (Probar) para asegurarse de que FMC se puede enlazar correctamente con el nombre de usuario y la contraseña del directorio proporcionados en el paso anterior.

Dado que estas pruebas se inician desde el FMC y no a través de una de las interfaces enrutables configuradas en el FTD (como interna, externa o dmz), una conexión correcta (o fallida) no garantiza el mismo resultado para la autenticación de AnyConnect porque las solicitudes de autenticación LDAP de AnyConnect se inician desde una de las interfaces enrutables del FTD.

Para obtener más información sobre la prueba de conexiones LDAP del FTD, revise las secciones Prueba de AAA y Captura de paquetes en el área de resolución de problemas.

Status



Test connection succeeded

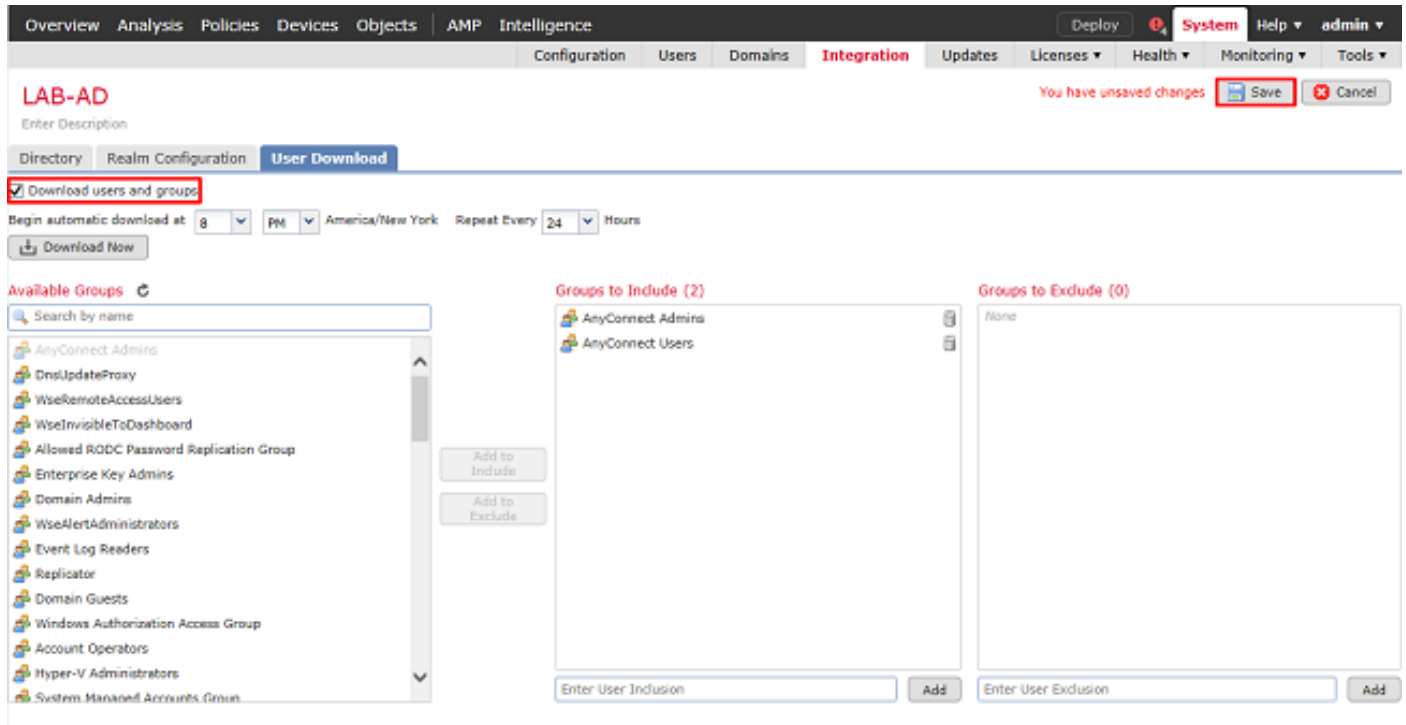
5. En User Download, descargue los grupos que se utilizan para la identidad del usuario en pasos posteriores.

Marque la casilla Descargar usuarios y grupos y la columna de Grupos disponibles se rellena con los grupos configurados en Active Directory.

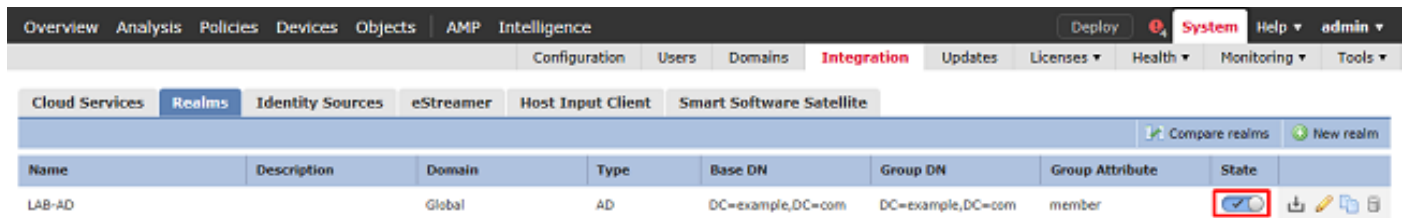
Los grupos pueden ser Incluidos o Excluidos; sin embargo, de forma predeterminada, se incluyen todos los grupos que se encuentran en el DN de grupo.

También se pueden incluir o excluir usuarios específicos. Los grupos y usuarios incluidos estarán disponibles para seleccionarlos posteriormente para la identidad del usuario.

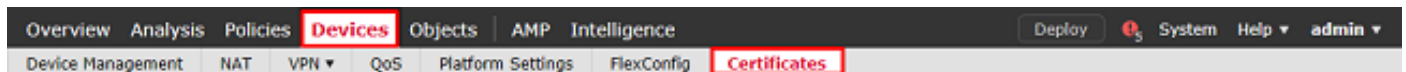
Cuando haya terminado, haga clic en Guardar.



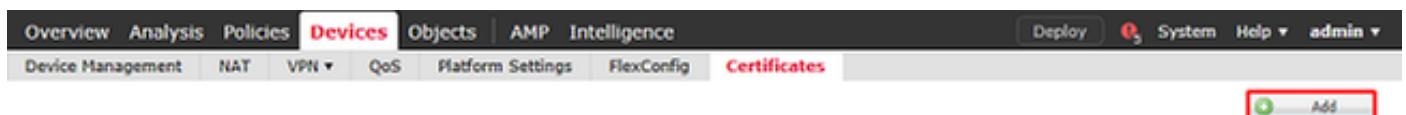
6. Active el nuevo rango.



7. Si se utiliza LDAPS o STARTTLS, el FTD también debe confiar en la CA raíz. Para hacer esto, primero navegue hasta Dispositivos > Certificados.



Haga clic en Agregar en la esquina superior derecha.



Seleccione el FTD, se añade la configuración LDAP a y, a continuación, haga clic en el símbolo + (más).

Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

FTD-2

Cert Enrollment*:

Select a certificate enrollment object



Add

Cancel

Dé un Nombre al punto de confianza y, a continuación, seleccione Inscripción manual en el menú desplegable Tipo de inscripción. Pegue aquí el certificado de CA raíz PEM y haga clic en Guardar.

Add Cert Enrollment



Name*

LDAPS_ROOT

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Certificate:*

```
-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhki
G9w0BAQsFADAd
MRswGQYDVQQDEExJeGFtcGxlVdJTjIwMTYtQ0EwIBcNMjAwNDI
3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTIaMB0xGzAZBgNVBAMTEmV4YW1wbGU
tV0lOMjAxNi1DQTCC
ASIWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719N
zSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPbf
d++M+bLn3AiZnHV
OO+k6dVVY/E5qVkeKSGoY+v940S2316lzdwrReMOFhgbc2qMertIo
ficrRhohonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN
O7KEMkfA1LPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBU
aLdQaabhipD/
sVs5PneYJX8YKma821uYI6i90YuytmsHBtCieyC062a8BKqOL7N86
```

Allow Overrides

Save


Cancel

Compruebe que el punto de confianza creado está seleccionado y haga clic en Agregar.

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*: 

Cert Enrollment Details:

Name: LDAPS_ROOT

Enrollment Type: Manual

SCEP URL: NA

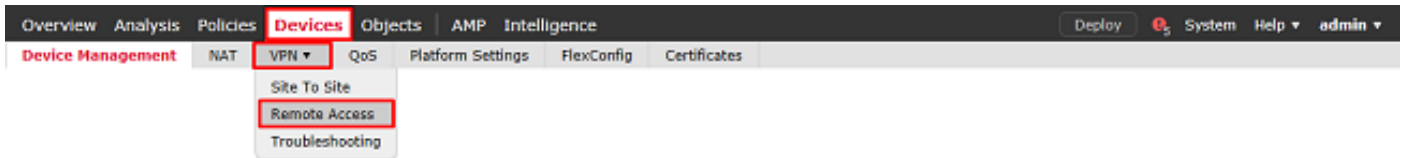
El nuevo punto de confianza aparece bajo el FTD. Aunque menciona que se requiere la importación del certificado de identidad, no es necesario que el FTD autentique el certificado SSL enviado por el servidor LDAPS. Por lo tanto, este mensaje puede ser ignorado.

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-PKCS12	Global	PKCS12 file	
FTD-2			
FTD-2-PKCS12	Global	PKCS12 file	
FTD-2-Selfsigned	Global	Self-Signed	
LDAPS_ROOT	Global	Manual	Identity certificate import required

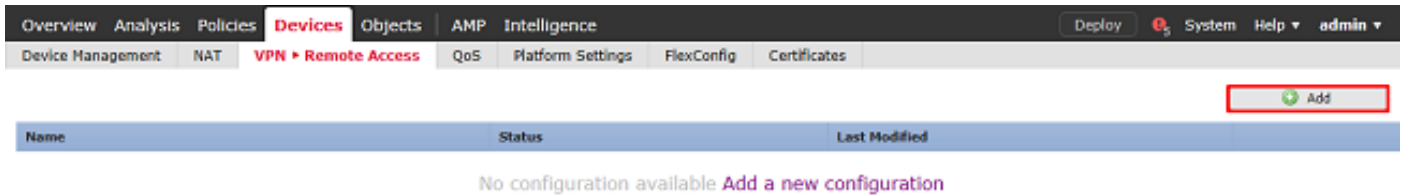
Configuración de AnyConnect para la autenticación de AD

1. En estos pasos se supone que no se ha creado ya ninguna directiva VPN de acceso remoto. Si se ha creado una, haga clic en el botón edit (editar) de dicha directiva y vaya directamente al paso 3.

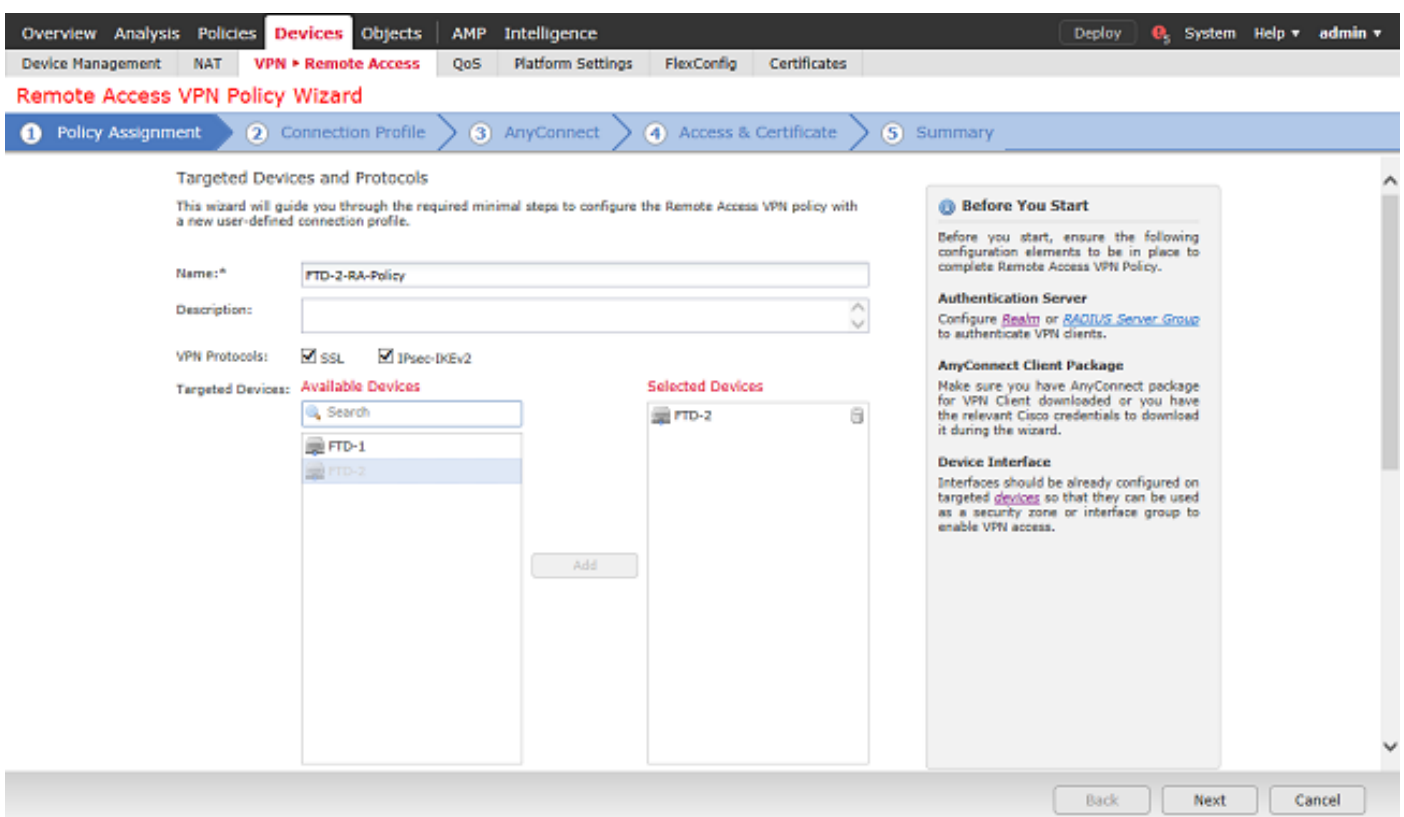
Vaya a Devices > VPN > Remote Access.



Haga clic en Agregar para crear una nueva Política VPN de acceso remoto



2. Complete el Asistente para directivas VPN de acceso remoto. En Asignación de directiva, especifique un nombre para la directiva y los dispositivos a los que se aplica la directiva.



En Perfil de conexión, especifique el nombre de Perfil de conexión que también se utiliza como alias de grupo que los usuarios de AnyConnect ven cuando se conectan.

Especifique el rango creado previamente en Servidor de autenticación.

Especifique el método mediante el cual se asignan direcciones IP a los clientes de AnyConnect.

Especifique la directiva de grupo predeterminada que se utiliza para este perfil de conexión.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 **Connection Profile** 3 AnyConnect 4 Access & Certificate 5 Summary

Connection Profile:
 Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name: *
This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):
 Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: (Realm or RADIUS)
 Authentication Server: * (RADIUS)
 Authorization Server: (RADIUS)
 Accounting Server: (RADIUS)

Client Address Assignment:
 Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (RADIUS only) ⓘ
 Use DHCP Servers
 Use IP Address Pools

IPv4 Address Pools: ⓘ
 IPv6 Address Pools: ⓘ

Group Policy:
 A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy: * ⓘ
[Edit Group Policy](#)

Back Next Cancel

En AnyConnect, cargue y especifique los paquetes de AnyConnect que se utilizan.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **AnyConnect** 4 Access & Certificate 5 Summary

AnyConnect Client Image
 The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#). [Show Re-order buttons](#) ⓘ

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	anyconnect-linux64-4.7.03052-we...	anyconnect-linux64-4.7.03052-webdeploy-k9...	Linux
<input checked="" type="checkbox"/>	anyconnect-win-4.7.00136-webde...	anyconnect-win-4.7.00136-webdeploy-k9.pkg	Windows

Back Next Cancel

En Acceso y certificado, especifique la interfaz a la que acceden los usuarios de AnyConnect para AnyConnect.

Cree y/o especifique el certificado que utiliza el FTD durante el intercambio de señales SSL.

Asegúrese de que la casilla de verificación Omitir la política de control de acceso para el tráfico descifrado (sysopt permit-vpn) esté desactivada para que la identidad de usuario creada más adelante surta efecto para las conexiones RAVPN.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Network Interface for Incoming VPN Access
 Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone: +

Enable DTLS on member interfaces

Device Certificates
 Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment: +

Enroll the selected certificate object on the target devices

Access Control for VPN Traffic
 All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Bypass Access Control policy for decrypted traffic (except permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Back Next Cancel

En Summary, revise la configuración y haga clic en Finish.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name: FTD-2-RA-Policy

Device Targets: FTD-2

Connection Profile: General

Connection Alias: General

AAA:

- Authentication Method: AAA Only
- Authentication Server: LAB-AD
- Authorization Server: -
- Accounting Server: -

Address Assignment:

- Address from AAA: -
- DHCP Servers: -
- Address Pools (IPv4): AnyConnect-Pool
- Address Pools (IPv6): -

Group Policy: DfltGrpPolicy

AnyConnect Images:

- anyconnect-linux64-4.7.03052-webdeploy-k9.pkg
- anyconnect-win-4.7.00136-webdeploy-k9.pkg

Interface Objects: outside-zone

Device Certificates: FTD-2-Selfsigned

Device Identity Certificate Enrollment

Certificate enrollment object 'FTD-2-Selfsigned' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update**
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- Port Configuration**
SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Anyconnect image download. NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.

Network Interface Configuration
 Make sure to add interface from targeted devices to SecurityZone object 'outside-zone'

Back Finish Cancel

3. En la directiva VPN > Acceso remoto, haga clic en el icono Edit (lápiz) para obtener el perfil de conexión correspondiente.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

FTD-2-RA-Policy Save Cancel

Enter Description Policy Assignments (1)

Connection Profile Access Interfaces **Advanced**

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DftGrpPolicy
General	Authentication: LAB-AD (AD) Authorization: None Accounting: None	DftGrpPolicy

Asegúrese de que el Servidor de autenticación esté configurado en el rango creado anteriormente.

En Advanced Settings, se puede marcar Enable Password Management para permitir que los usuarios cambien su contraseña cuando o antes de que caduque.

Sin embargo, esta configuración requiere que el rango utilice LDAPS. Si se ha realizado algún cambio, haga clic en Guardar.

Edit Connection Profile

Connection Profile:*

Group Policy:* [Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method:

Authentication Server:

Use secondary authentication

Authorization

Authorization Server:

Allow connection only if user exists in authorization database

Accounting

Accounting Server:

Advanced Settings

Strip Realm from username

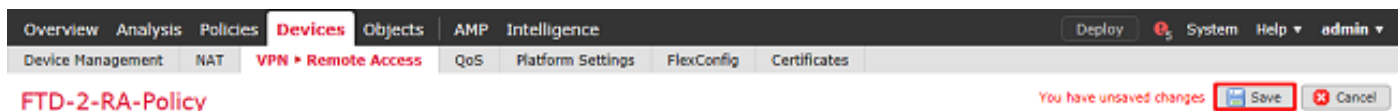
Strip Group from username

Enable Password Management

Notify User days prior to password expiration

Notify user on the day of password expiration

Cuando haya terminado, haga clic en Guardar.

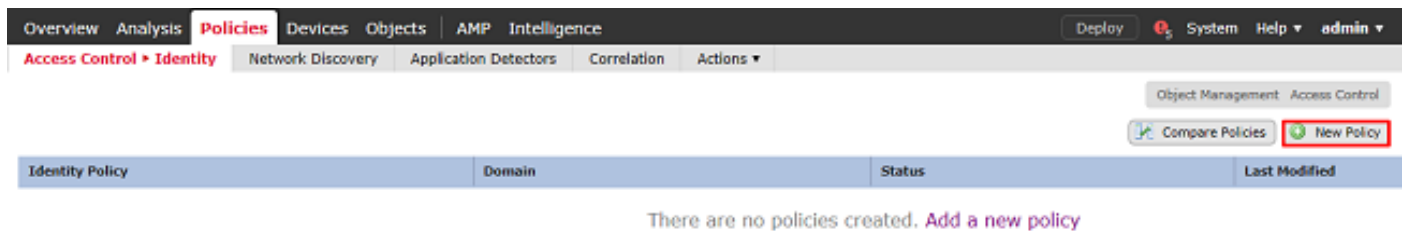


Habilitar la política de identidad y configurar las políticas de seguridad para la identidad del usuario

1. Vaya a Políticas > Control de acceso > Identidad.



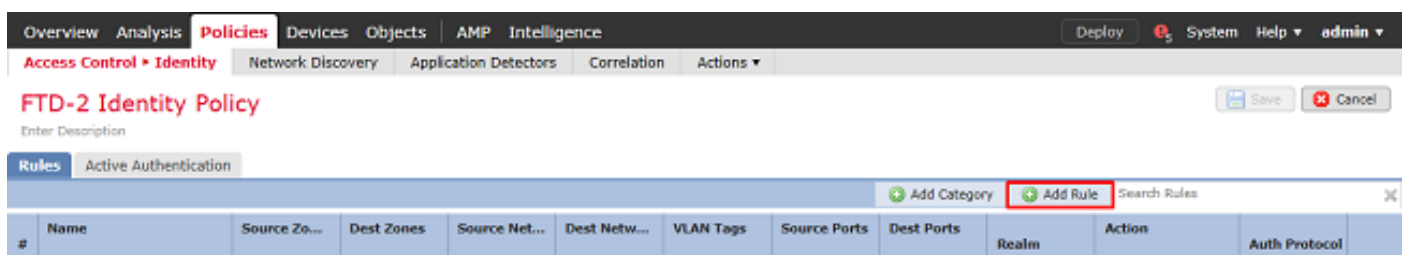
Cree una nueva política de identidad.



Especifique un nombre para la nueva política de identidad.



2. Haga clic en Agregar regla.



3. Especifique un nombre para la nueva regla. Asegúrese de que esté habilitado y de que la acción esté configurada como Autenticación Pasiva.

Haga clic en la pestaña Rango y configuración y seleccione el rango creado anteriormente. Haga clic en Agregar cuando haya terminado.

Add Rule

Name: Enabled

Insert:

Action: Realm: LAB-AD (AD) Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None

Remote access VPN sessions are actively authenticated by VPN. Other sessions use the rule Action.

Zones Networks VLAN Tags Ports Realm & Settings

Realm * Use active authentication if passive or VPN identity cannot be established

* Required Field

4. Haga clic en Guardar.

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help admin

Access Control > Identity Network Discovery Application Detectors Correlation Actions

FTD-2 Identity Policy

Enter Description You have unsaved changes

Rules Active Authentication Add Category Add Rule Search Rules

#	Name	Source Zo...	Dest Zones	Source Net...	Dest Netw...	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules											
This category is empty											
Standard Rules											
1	RAVPN	any	any	any	any	any	any	any	LAB-AD	Passive Authentication	none
Root Rules											
This category is empty											

Displaying 1 - 1 of 1 rules |< < Page 1 of 1 >> |>

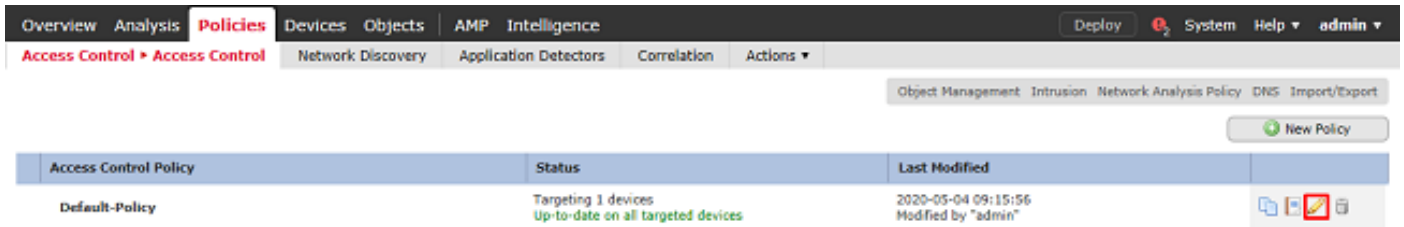
5. Acceda a Políticas > Control de Acceso > Control de Acceso.

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help admin

Access Control > Identity Network Discovery Application Detectors Correlation Actions

- Access Control
- Intrusion
- Malware & File
- DNS
- Identity**
- SSL
- Prefilter

6. Edite la política de control de acceso en la que se ha configurado el FTD.



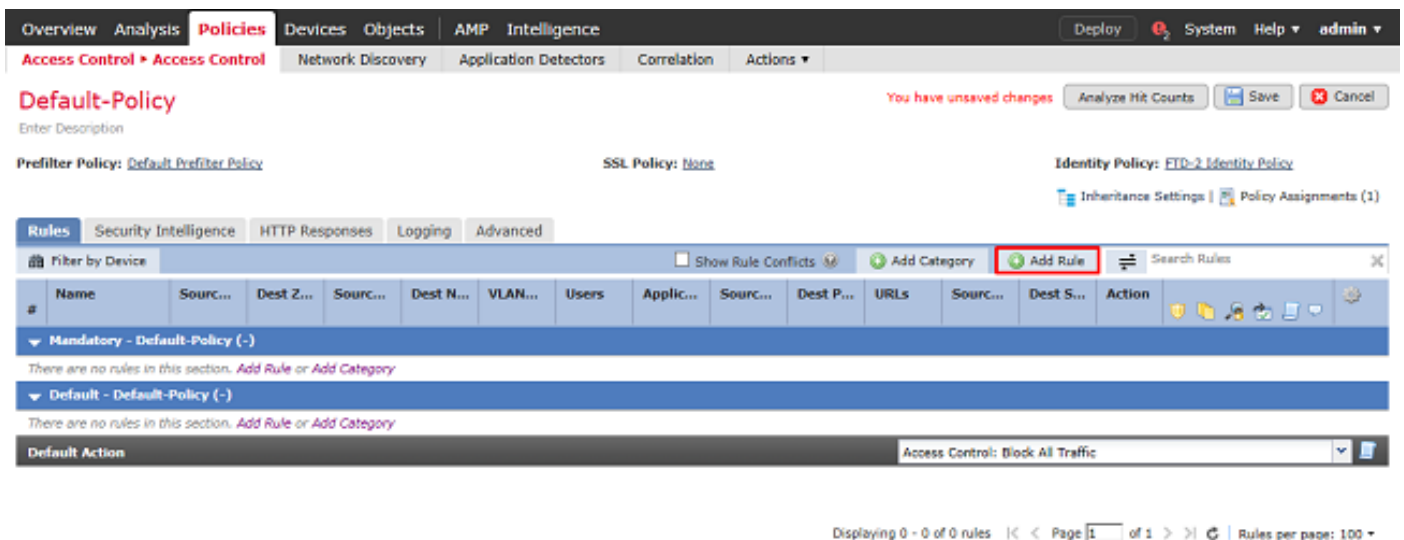
7. Haga clic en el valor junto a Política de identidad.



Seleccione la política de identidad creada anteriormente y haga clic en Aceptar.



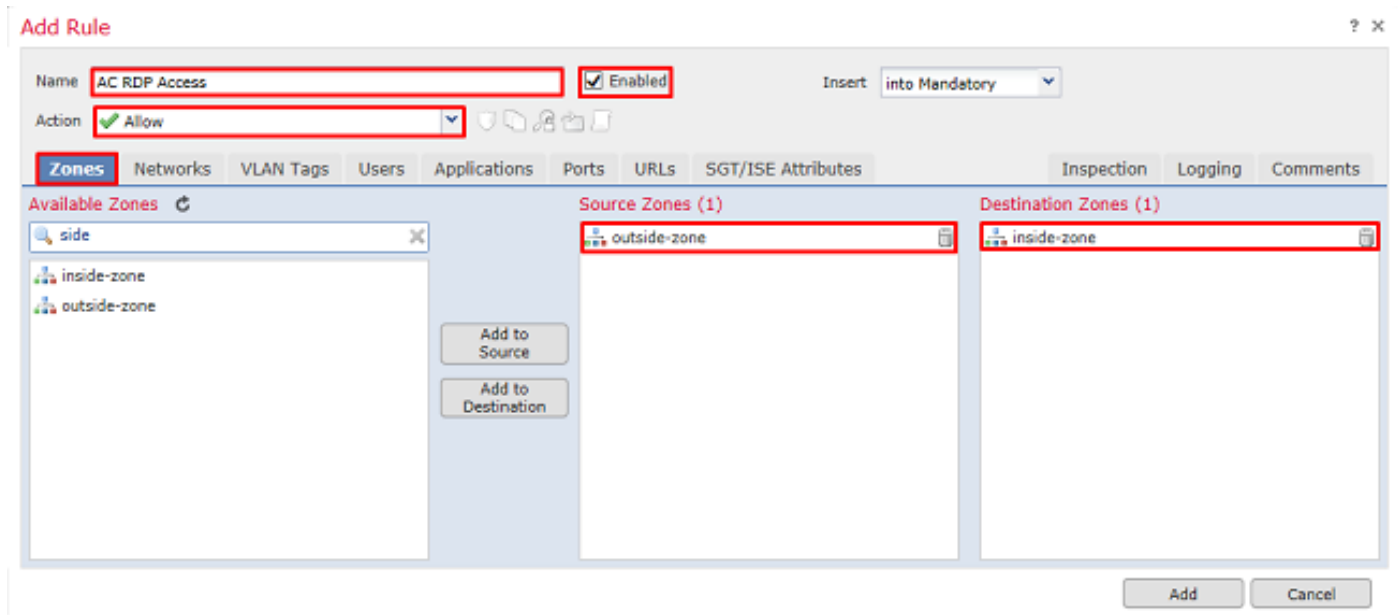
8. Haga clic en Agregar Regla para crear una nueva regla de ACP. Estos pasos crean una regla para permitir que el usuario dentro del grupo de administradores de AnyConnect se conecte a los dispositivos dentro de la red interna mediante RDP.



Especifique un nombre para la regla. Asegúrese de que la regla esté Habilitada y que tenga la Acción apropiada.

En la pestaña Zonas, especifique las zonas apropiadas para el tráfico interesante.

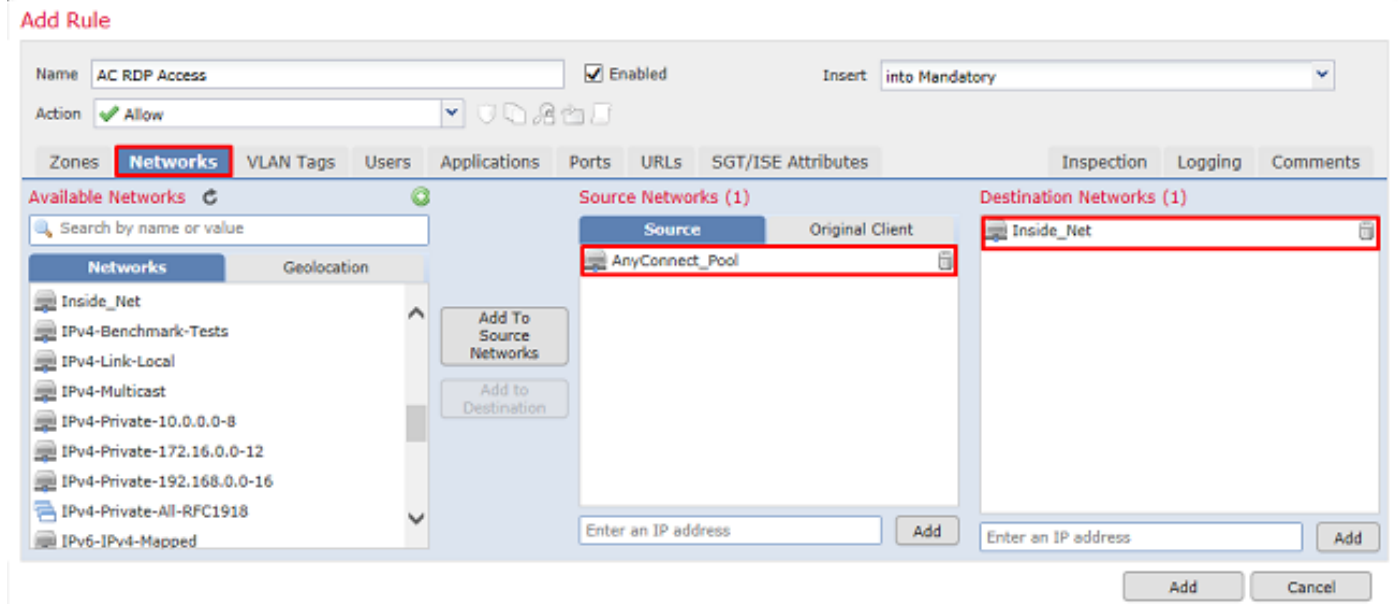
El tráfico RDP iniciado por los usuarios entra al FTD originado en la interfaz de la zona exterior y sale de la zona interior.



En Redes, defina las redes de origen y de destino.

El objeto AnyConnect_Pool incluye las direcciones IP asignadas a los clientes de AnyConnect.

El objeto Inside_Net incluye la subred interna de la red.

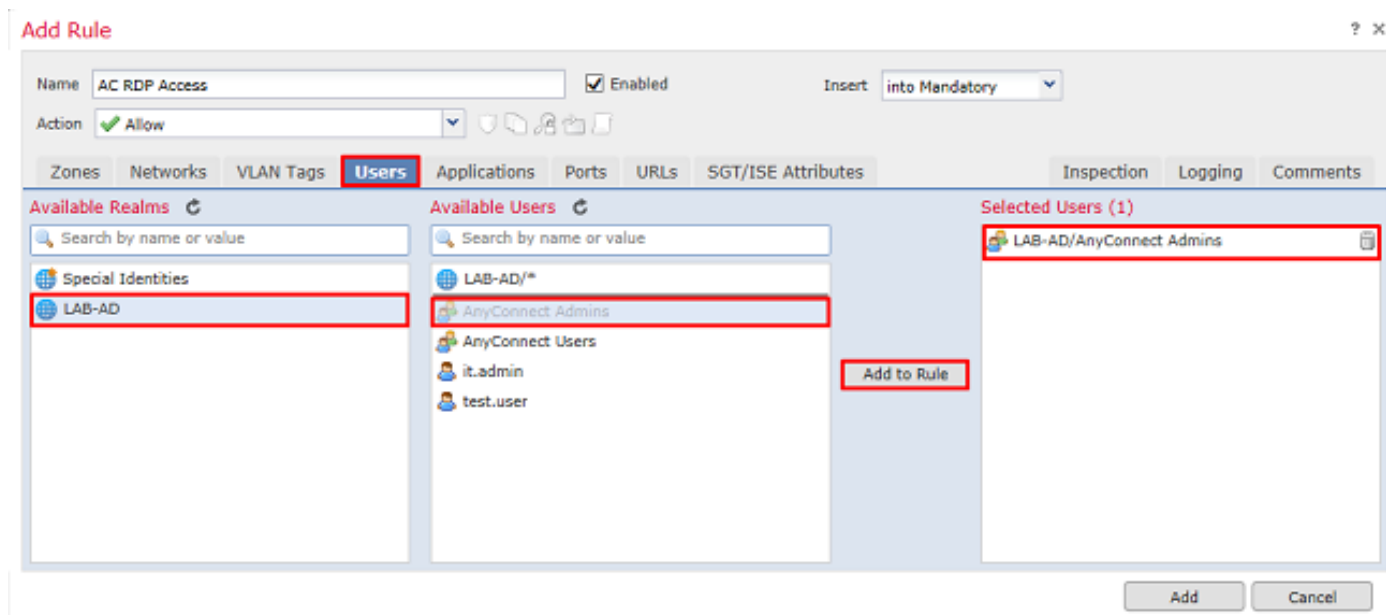


En Usuarios, haga clic en el rango creado anteriormente en Rangos Disponibles, haga clic en el grupo o usuario apropiado en Usuarios Disponibles, luego haga clic en Agregar a Regla.

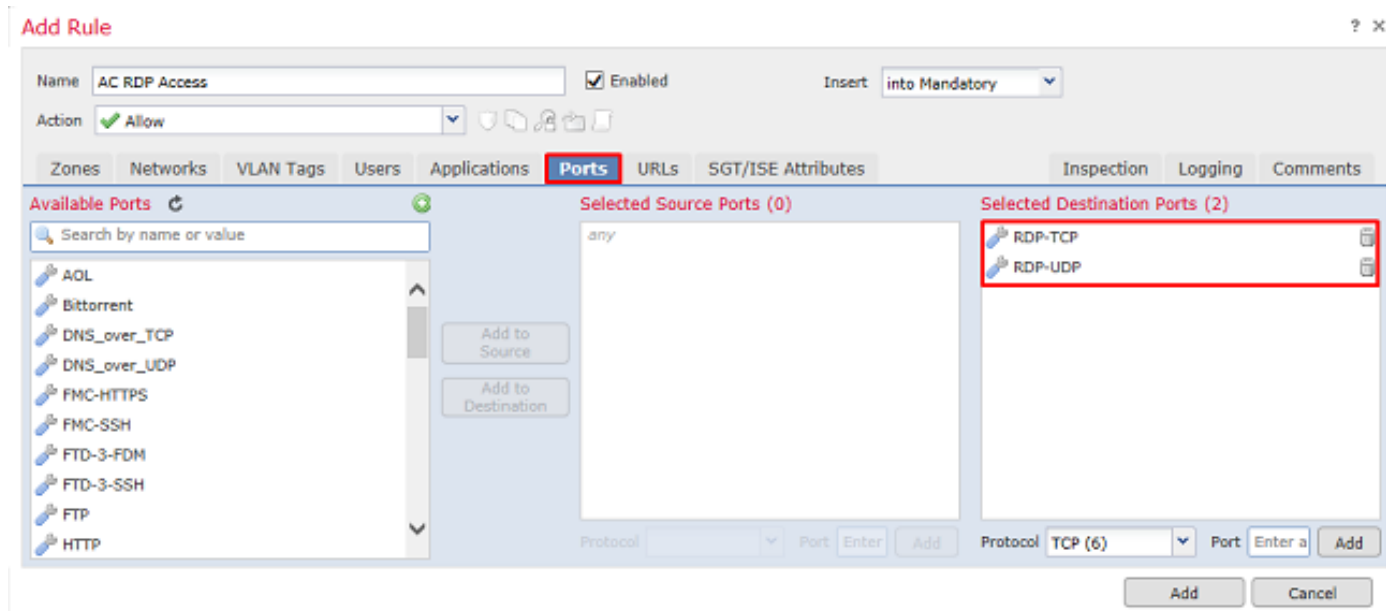
Si no hay usuarios o grupos disponibles en la sección Usuarios Disponibles, asegúrese de que FMC descargó los Usuarios y los Grupos en la sección de rango y de que se incluyen los Grupos/Usuarios adecuados.

El usuario/grupo especificado aquí se comprueba desde la perspectiva de origen.

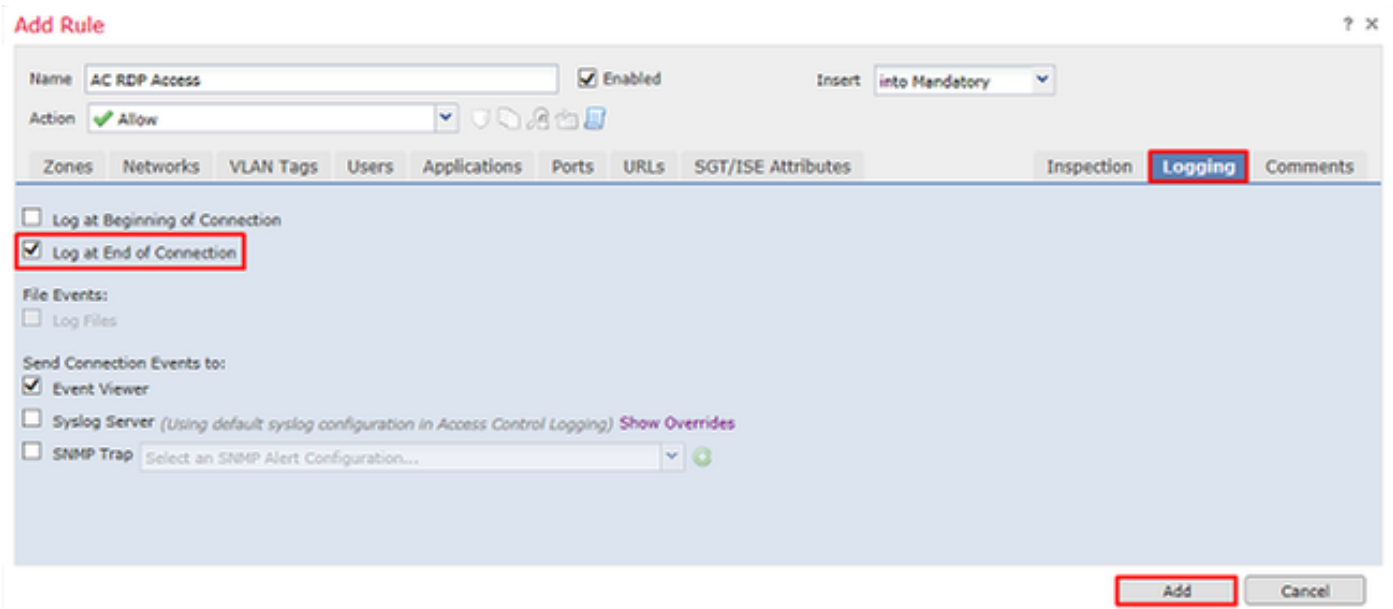
Por ejemplo, con lo que se ha definido hasta ahora en esta regla, el FTD evalúa que el tráfico se origina en la zona exterior y se destina a la zona interior, se origina en la red en el objeto AnyConnect_Pools y se destina a la red en el objeto Inside_Net, y el tráfico se origina en un usuario del grupo de administradores de AnyConnect.



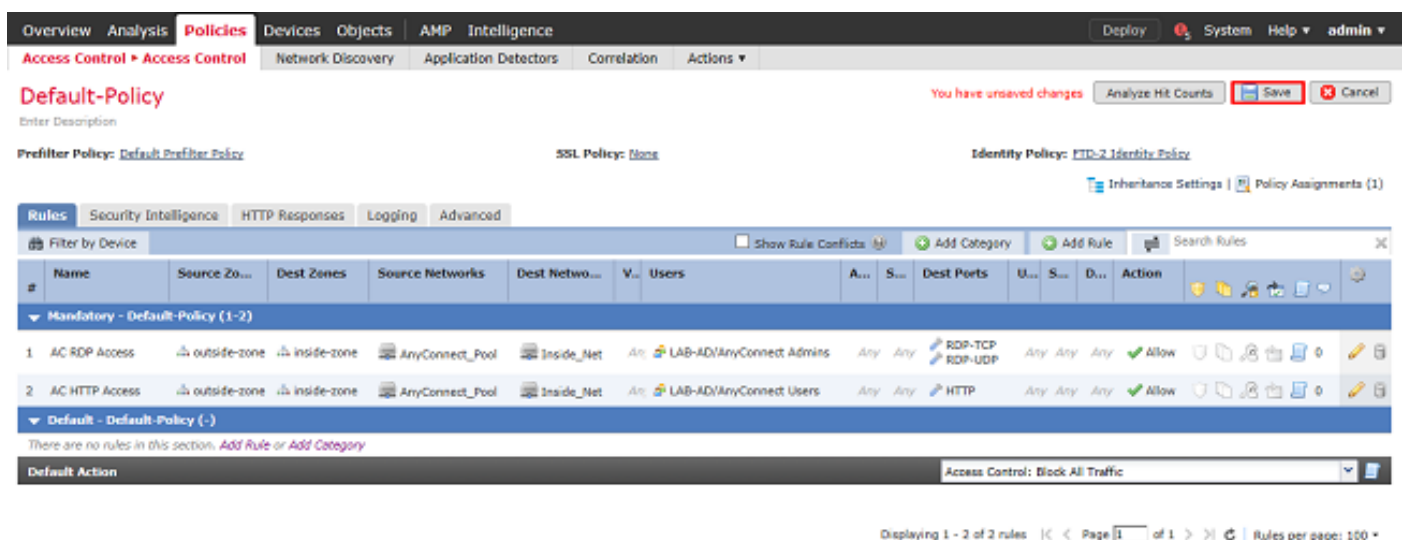
En Puertos, se crearon y agregaron objetos RDP personalizados para permitir el puerto TCP y UDP 3389. Observe que RDP podría haber sido agregado bajo la sección Aplicaciones, pero por simplicidad, sólo se verifican los puertos.



Por último, asegúrese de que en Registro, Registro al final de la conexión se verifique más adelante para obtener una verificación adicional. Haga clic en Agregar cuando haya terminado.



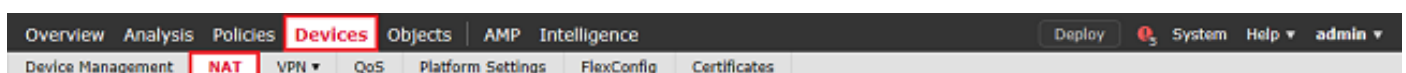
9. Se crea una regla adicional para el acceso HTTP a fin de permitir a los usuarios del grupo AnyConnect User el acceso al sitio web de Windows Server IIS. Click Save.



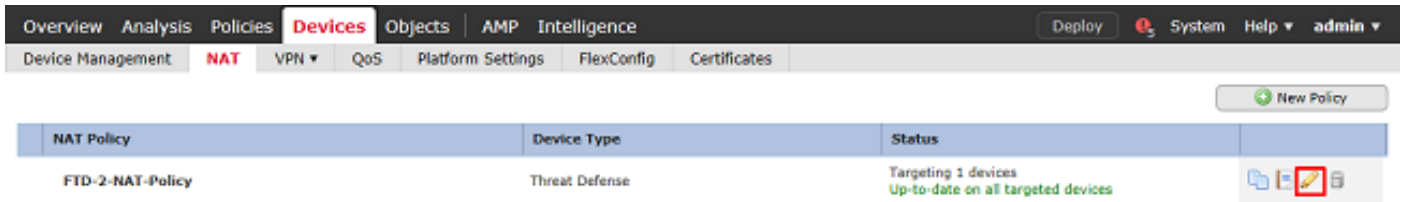
Configurar exención de NAT

Si hay reglas NAT que afectan al tráfico de AnyConnect, como las reglas PAT de Internet, es importante configurar reglas de exención NAT para que el tráfico de AnyConnect no se vea afectado por NAT.

1. Vaya a Devices > NAT.

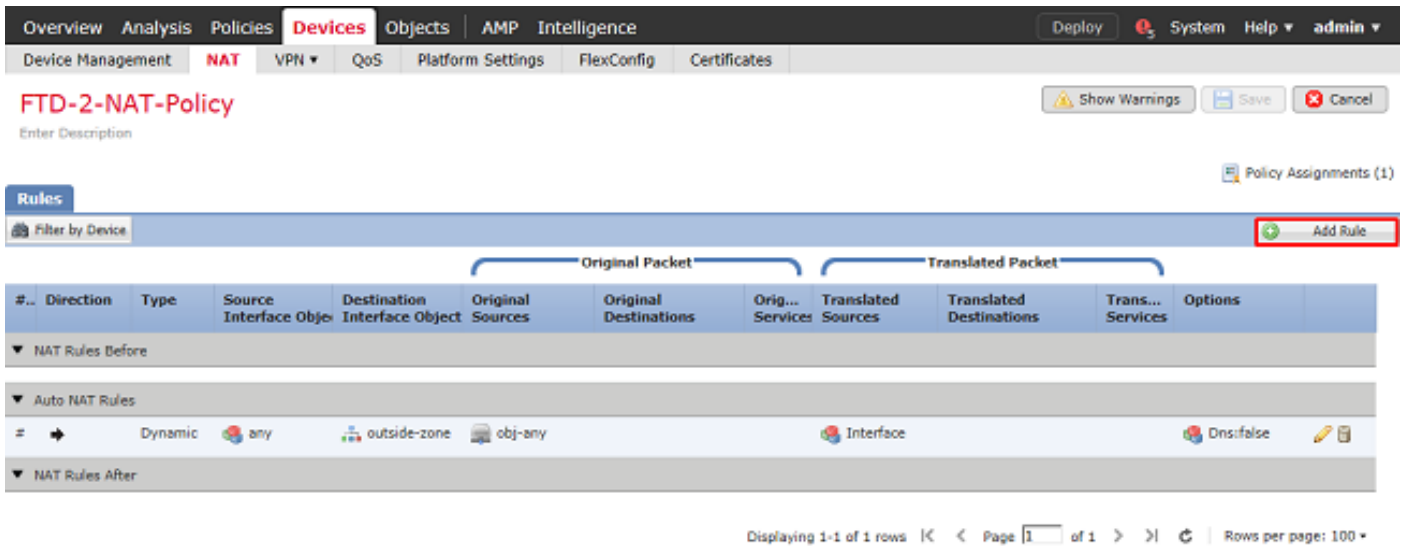


Seleccione la política NAT aplicada al FTD.



2. En esta política NAT, hay una PAT dinámica al final que afecta a todo el tráfico (incluido el tráfico de AnyConnect) que egresa de la interfaz externa a la interfaz externa.

Para evitar que el tráfico de AnyConnect se vea afectado por NAT, haga clic en Agregar regla.



3. Configure una regla de exención de NAT, asegúrese de que la regla sea una regla de NAT manual con tipo estático. Esta es una regla NAT bidireccional que se aplica al tráfico de AnyConnect.

Con esta configuración, cuando el FTD detecta tráfico originado en Inside_Net y destinado a la dirección IP de AnyConnect (definida por AnyConnect_Pool), el origen se traduce al mismo valor (Inside_Net) y el destino se traduce al mismo valor (AnyConnect_Pool) cuando el tráfico ingresa en inside_zone y egresa de outside_zone. Básicamente, esto omite la NAT cuando se cumplen estas condiciones.

Add NAT Rule ? X

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects Translation PAT Pool Advanced

Available Interface Objects ↻

- inside-zone
- outside-zone

Add to Source

Add to Destination

Source Interface Objects (1)

■ inside-zone

Destination Interface Objects (1)

■ outside-zone

OK Cancel

Add NAT Rule ? X

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet

Original Source:* Inside_Net +

Original Destination: Address

AnyConnect_Pool +

Original Source Port: +

Original Destination Port: +

Translated Packet

Translated Source: Address

Inside_Net +

Translated Destination: AnyConnect_Pool +

Translated Source Port: +

Translated Destination Port: +

OK Cancel

Además, el FTD está configurado para realizar una búsqueda de ruta en este tráfico y no en el ARP proxy. Haga clic en Aceptar cuando haya terminado.

Add NAT Rule ? X

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Falthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

4. Haga clic en Guardar.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy ! System Help admin

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates

FTD-2-NAT-Policy You have unsaved changes

Enter Description Policy Assignments (1)

Rules

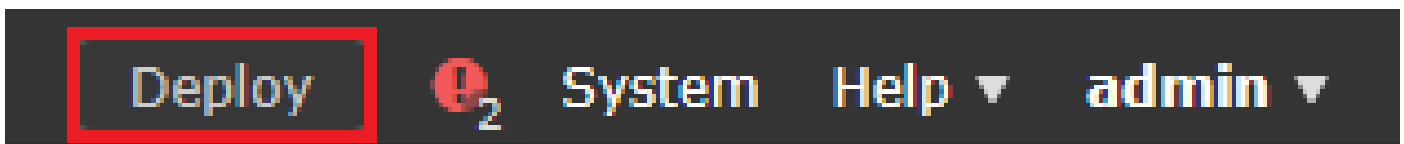
Filter by Device Add Rule

#	Direction	Type	Original Packet		Translated Packet		Trans... Services	Options
			Source Interface Obj	Destination Interface Object	Original Sources	Original Destinations		
▼ NAT Rules Before								
1	↔	Static	inside-zone	outside-zone	Inside_Net	AnyConnect_Pool	Inside_Net AnyConnect_Pool	Dns:false route-lookup no-proxy-arp
▼ Auto NAT Rules								
#	↔	Dynamic	any	outside-zone	obj-any		Interface	Dns:false
▼ NAT Rules After								

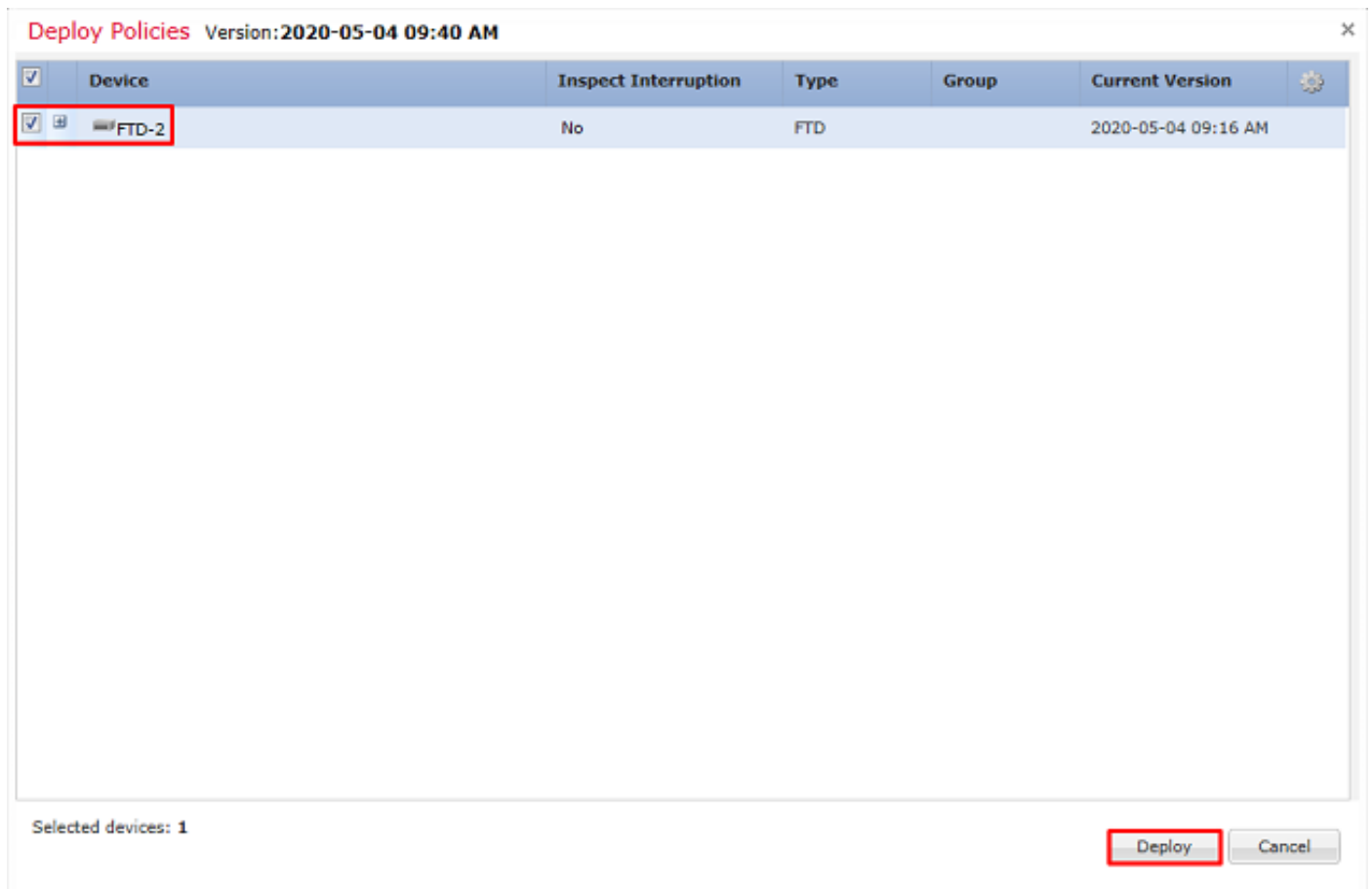
Displaying 1-2 of 2 rows | Page 1 of 1 | Rows per page: 100

Implementación

1. Una vez finalizada la configuración, haga clic en Deploy.



2. Haga clic en la casilla de verificación junto al FTD al que se le aplica la configuración y, a continuación, haga clic en Desplegar.



Verificación

Configuración final

Configuración AAA

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
max-failed-attempts 4
realm-id 5
aaa-server LAB-AD host win2016.example.com
server-port 389
ldap-base-dn DC=example,DC=com
ldap-group-base-dn DC=example,DC=com
ldap-scope subtree
ldap-naming-attribute samaccountname
ldap-login-password *****
ldap-login-dn ftd.admin@example.com
server-type microsoft
```

Configuración de AnyConnect

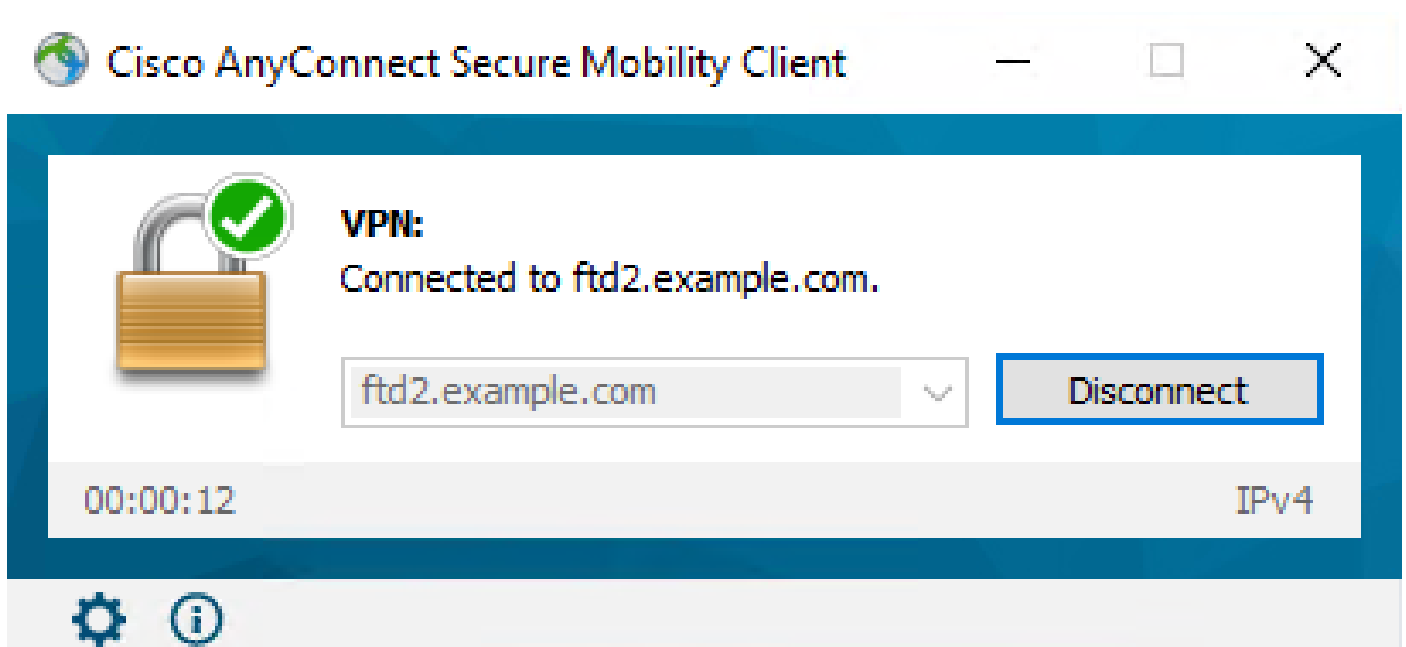
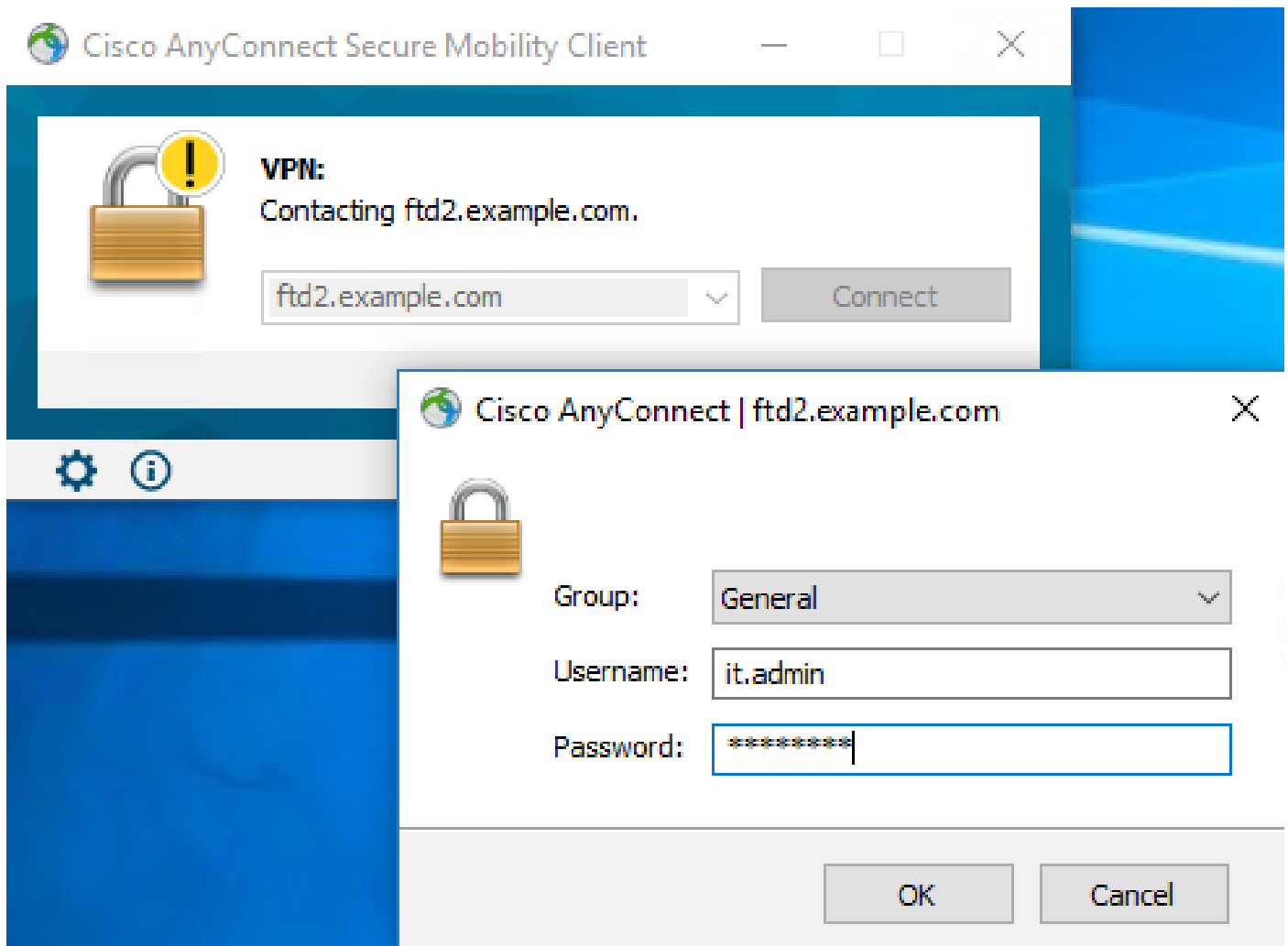
```
> show running-config webvpn
webvpn
  enable Outside
  anyconnect image disk0:/csm/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1 regex "Linux"
  anyconnect image disk0:/csm/anyconnect-win-4.7.00136-webdeploy-k9.pkg 2 regex "Windows"
  anyconnect profiles Lab disk0:/csm/lab.xml
  anyconnect enable
  tunnel-group-list enable
  cache
    no disable
  error-recovery disable

> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
  address-pool AnyConnect-Pool
  authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
  group-alias General enable

> show running-config group-policy
group-policy DfltGrpPolicy attributes
  vpn-simultaneous-logins 10
  vpn-tunnel-protocol ikev2 ssl-client
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value Lab
  user-authentication-idle-timeout none
webvpn
  anyconnect keep-installer none
  anyconnect modules value dart
  anyconnect ask none default anyconnect
  http-comp none
  activex-relay disable
  file-entry disable
  file-browsing disable
  url-entry disable
  deny-message none
  anyconnect ssl df-bit-ignore enable

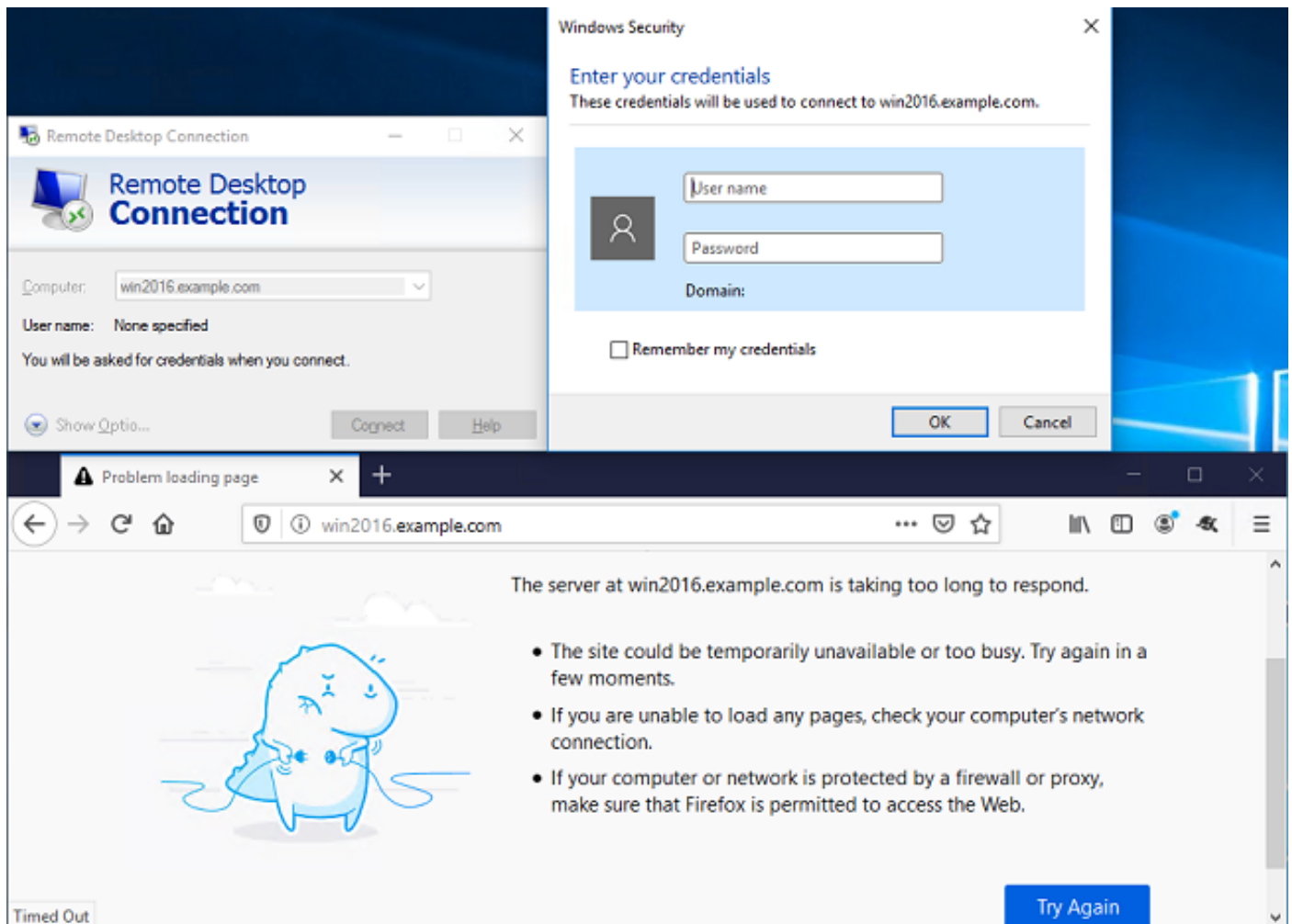
> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside
```

Conexión con AnyConnect y verificación de las reglas de la política de control de acceso

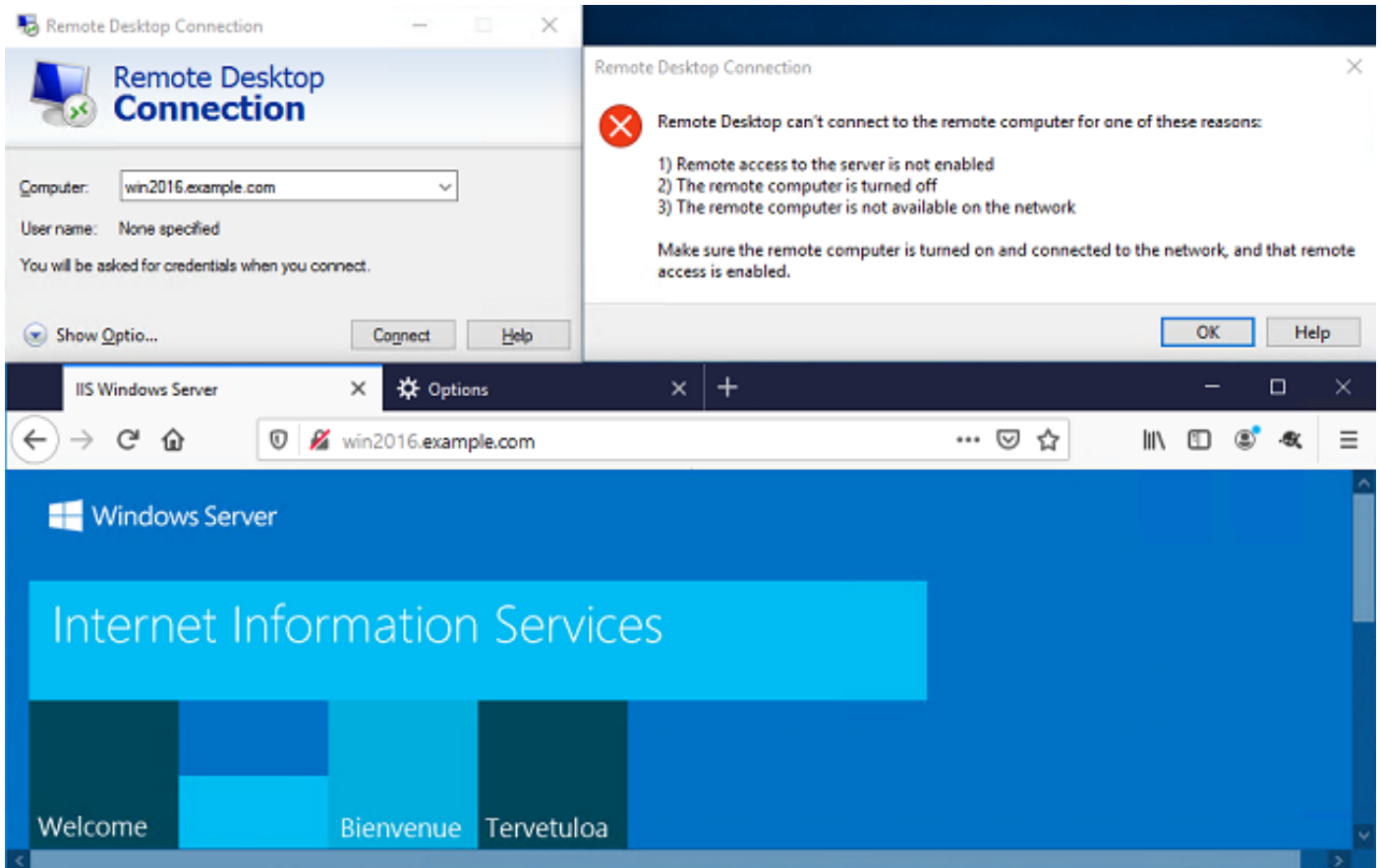


El usuario IT Admin pertenece al grupo AnyConnect Admins que tiene acceso RDP a Windows Server. Sin embargo, no tiene acceso a HTTP.

Al abrir una sesión de RDP y Firefox en este servidor, se comprueba que este usuario solo puede acceder al servidor a través de RDP.



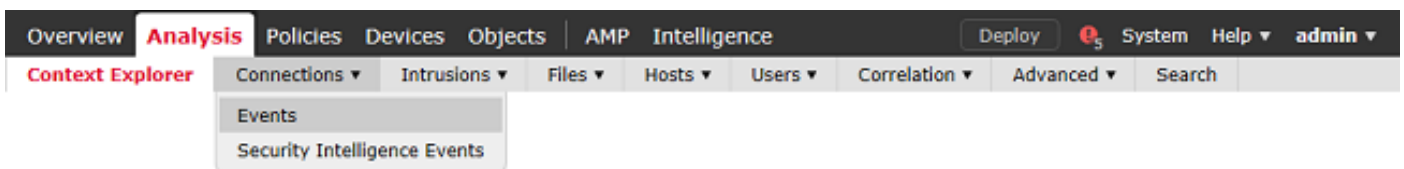
Si ha iniciado sesión con un usuario de prueba que pertenece al grupo Usuarios de AnyConnect que tiene acceso HTTP pero no acceso RDP, puede comprobar que las reglas de la directiva de control de acceso están surtiendo efecto.



Verificar con eventos de conexión FMC

Dado que el registro estaba habilitado en las reglas de la política de control de acceso, se pueden verificar los eventos de conexión para cualquier tráfico que coincida con esas reglas.

Vaya a Análisis > Conexiones > Eventos.



En la Vista de tabla de eventos de conexión, los registros se filtran para mostrar solamente los eventos de conexión para el administrador de TI.

Aquí puede verificar que se permite el tráfico RDP al servidor (TCP y UDP 3389); sin embargo, el tráfico del puerto 80 está bloqueado.

	Action	Initiator IP	Initiator User	Responder IP	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
<input type="checkbox"/>	Allow	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62473 / tcp	3389 / tcp
<input type="checkbox"/>	Block	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62474 / tcp	80 (http) / tcp
<input type="checkbox"/>	Block	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62475 / tcp	80 (http) / tcp
<input type="checkbox"/>	Block	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62476 / tcp	80 (http) / tcp

Para el usuario Test User, puede verificar que el tráfico RDP al servidor esté bloqueado y que el tráfico del puerto 80 esté permitido.

	Action	Initiator IP	Initiator User	Responder IP	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
<input type="checkbox"/>	Block	10.10.10.1	test user (LAB-AD\test.user, LDAP)	192.168.1.1	outside-zone	inside-zone	62493 / tcp	3389 / tcp
<input type="checkbox"/>	Allow	10.10.10.1	test user (LAB-AD\test.user, LDAP)	192.168.1.1	outside-zone	inside-zone	62494 / tcp	80 (http) / tcp

Troubleshoot

Depuraciones

Esta depuración se puede ejecutar en la CLI de diagnóstico para resolver problemas relacionados con la autenticación LDAP: debug ldap 255.

Para resolver problemas de la política de control de acceso de la identidad del usuario, system support firewall-engine-debug se puede ejecutar en clish para determinar por qué se permite o bloquea el tráfico inesperadamente.

Depuraciones de LDAP en funcionamiento

```
[53] Session Start
[53] New request Session, context 0x00002b1d13f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
```

```
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
      Base DN = [DC=example,DC=com]
      Filter  = [sAMAccountName=it.admin]
      Scope   = [SUBTREE]
[53] User DN = [CN=IT Admin,CN=Users,DC=example,DC=com]
[53] Talking to Active Directory server 192.168.1.1
[53] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[53] Read bad password count 6
[53] Binding as it.admin
[53] Performing Simple authentication for it.admin to 192.168.1.1
[53] Processing LDAP response for user it.admin
[53] Message (it.admin):
[53] Authentication successful for it.admin to 192.168.1.1
[53] Retrieved User Attributes:
[53]   objectClass: value = top
[53]   objectClass: value = person
[53]   objectClass: value = organizationalPerson
[53]   objectClass: value = user
[53]   cn: value = IT Admin
[53]   sn: value = Admin
[53]   givenName: value = IT
[53]   distinguishedName: value = CN=IT Admin,CN=Users,DC=example,DC=com
[53]   instanceType: value = 4
[53]   whenCreated: value = 20200421025811.0Z
[53]   whenChanged: value = 20200421204622.0Z
[53]   displayName: value = IT Admin
[53]   uSNCreated: value = 25896
[53]   memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
[53]   uSNChanged: value = 26119
[53]   name: value = IT Admin
[53]   objectGUID: value = &...J..0..2w...c
[53]   userAccountControl: value = 512
[53]   badPwdCount: value = 6
[53]   codePage: value = 0
[53]   countryCode: value = 0
[53]   badPasswordTime: value = 132320354378176394
[53]   lastLogoff: value = 0
[53]   lastLogon: value = 0
[53]   pwdLastSet: value = 132319114917186142
[53]   primaryGroupID: value = 513
[53]   objectSid: value = .....{I...;.....}j...
[53]   accountExpires: value = 9223372036854775807
[53]   logonCount: value = 0
[53]   sAMAccountName: value = it.admin
[53]   sAMAccountType: value = 805306368
[53]   userPrincipalName: value = it.admin@example.com
[53]   objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=example,DC=com
[53]   dSCorePropagationData: value = 16010101000000.0Z
[53]   lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End
```

No se puede establecer una conexión con el servidor LDAP

<#root>

[-2147483611] Session Start

```
[-2147483611] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483611] Fiber started
[-2147483611] Creating LDAP context with uri=ldap://171.16.1.1:389
[-2147483611]
```

```
Connect to LDAP server: ldap://172.16.1.1:389, status = Failed
```

```
[-2147483611] Unable to read rootDSE. Can't contact LDAP server.
[-2147483611] Fiber exit Tx=0 bytes Rx=0 bytes, status=-2
[-2147483611] Session End
```

Soluciones potenciales:

- Verifique el ruteo y asegúrese de que el FTD esté recibiendo una respuesta del servidor LDAP.
- Si se utiliza LDAPS o STARTTLS, asegúrese de que el certificado de CA raíz correcto sea de confianza para que el intercambio de señales SSL pueda completarse correctamente.
- Verifique que se utilicen la dirección IP y el puerto correctos. Si se utiliza un nombre de host, verifique que DNS pueda resolverlo a la dirección IP correcta.

Enlace DN de inicio de sesión o contraseña incorrecta

<#root>

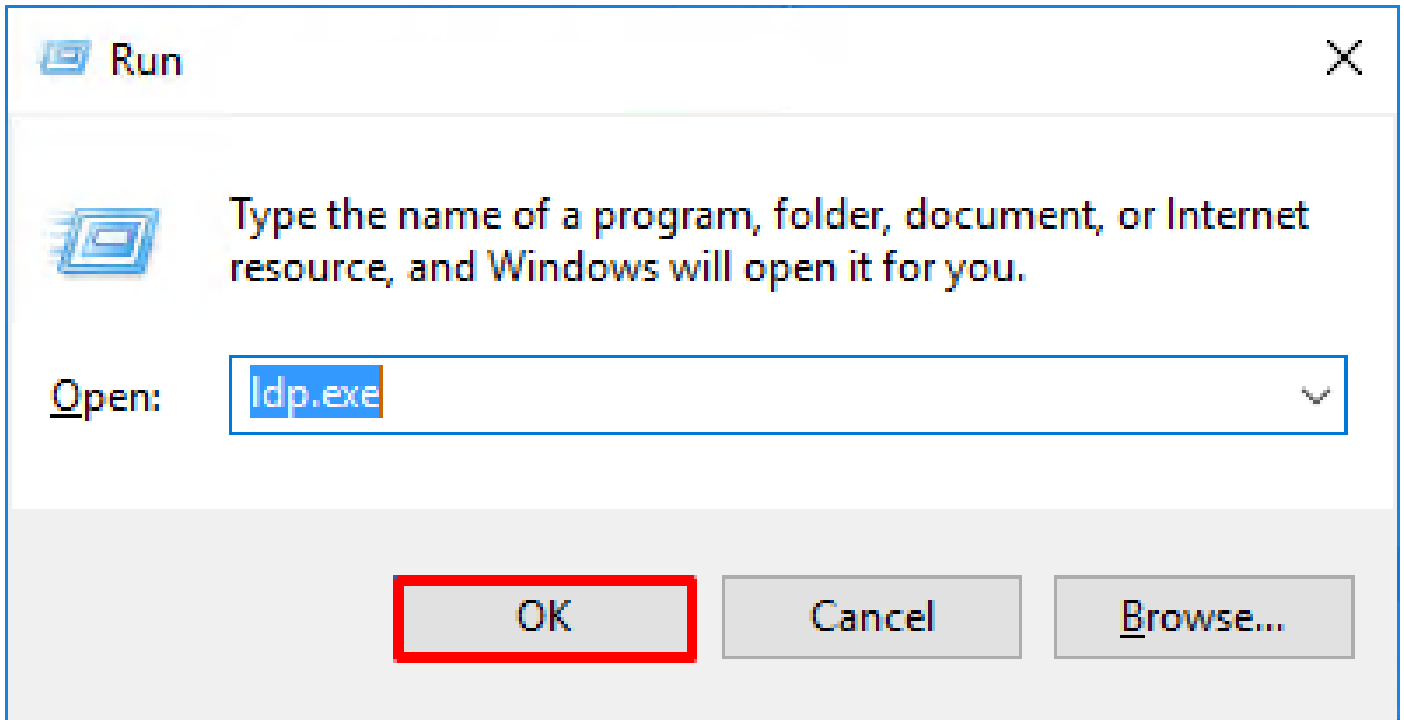
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] defaultNamingContext: value = DC=example,DC=com
[-2147483615] supportedLDAPVersion: value = 3
[-2147483615] supportedLDAPVersion: value = 2
[-2147483615] LDAP server 192.168.1.1 is Active directory
[-2147483615] supportedSASLMechanisms: value = GSSAPI
[-2147483615] supportedSASLMechanisms: value = GSS-SPNEGO
[-2147483615] supportedSASLMechanisms: value = EXTERNAL
[-2147483615] supportedSASLMechanisms: value = DIGEST-MD5
[-2147483615] Binding as ftd.admin@example.com
[-2147483615] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483615] Simple authentication for ftd.admin@example.com returned code (49) Invalid credentials
[-2147483615]
```

```
Failed to bind as administrator returned code (-1) Can't contact LDAP server
```

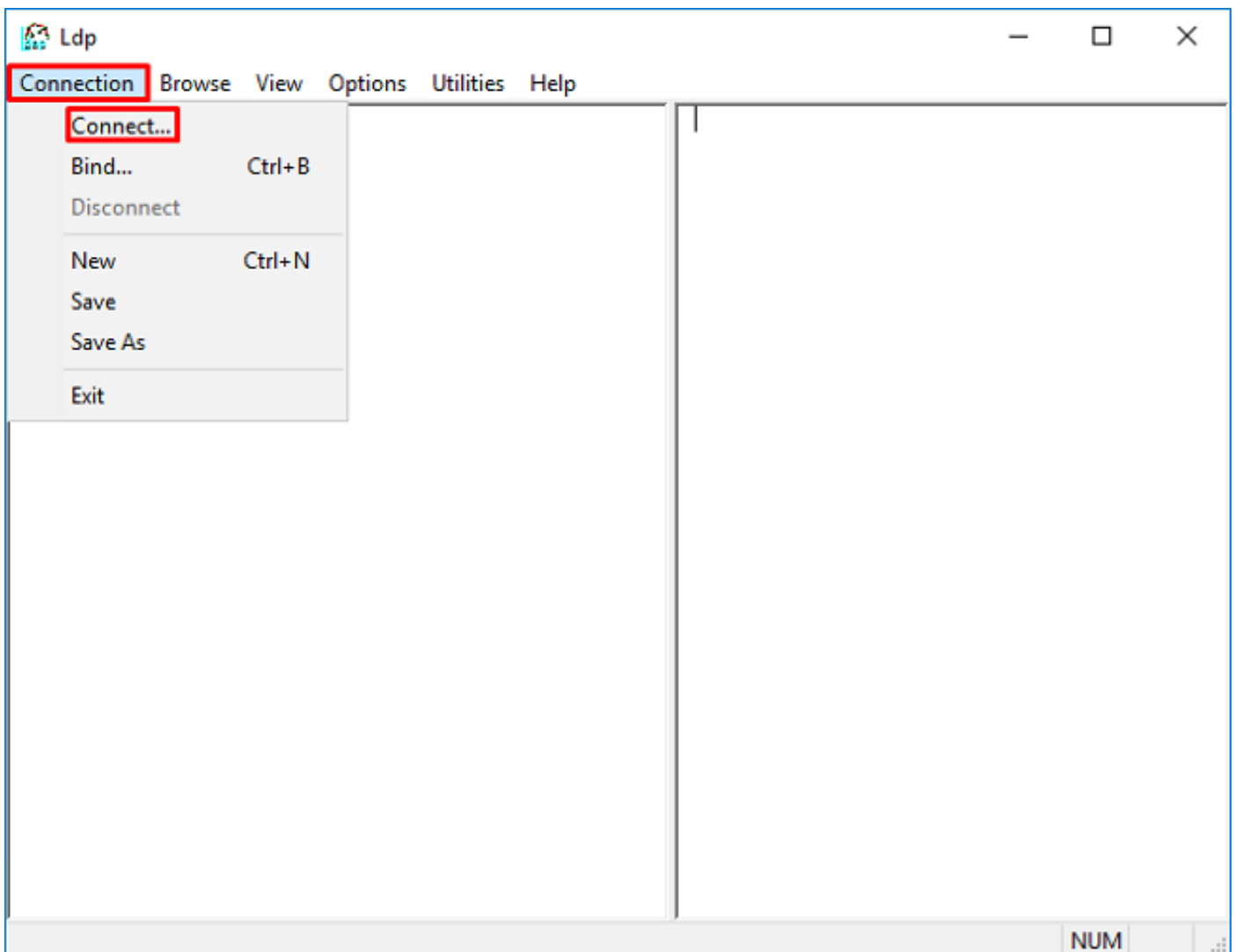
```
[-2147483615] Fiber exit Tx=186 bytes Rx=744 bytes, status=-2
[-2147483615] Session End
```

Solución potencial: compruebe que el DN de inicio de sesión y la contraseña de inicio de sesión estén configurados correctamente. Esto se puede verificar en el servidor de AD con ldp.exe. Para verificar que una cuenta puede enlazar con éxito usando ldp, siga estos pasos:

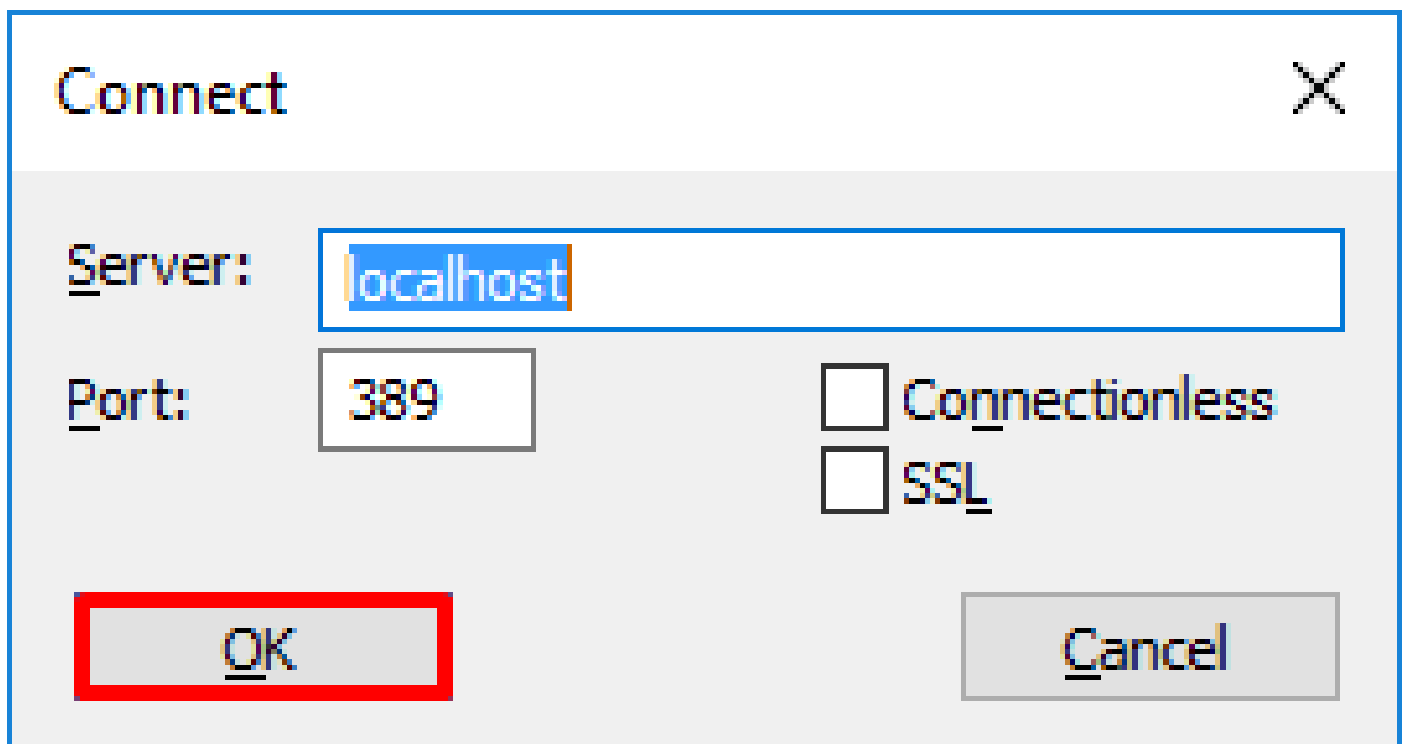
1. En el servidor de AD, presione Win+R y busque ldp.exe



2. En Conexión, seleccione Conectar.



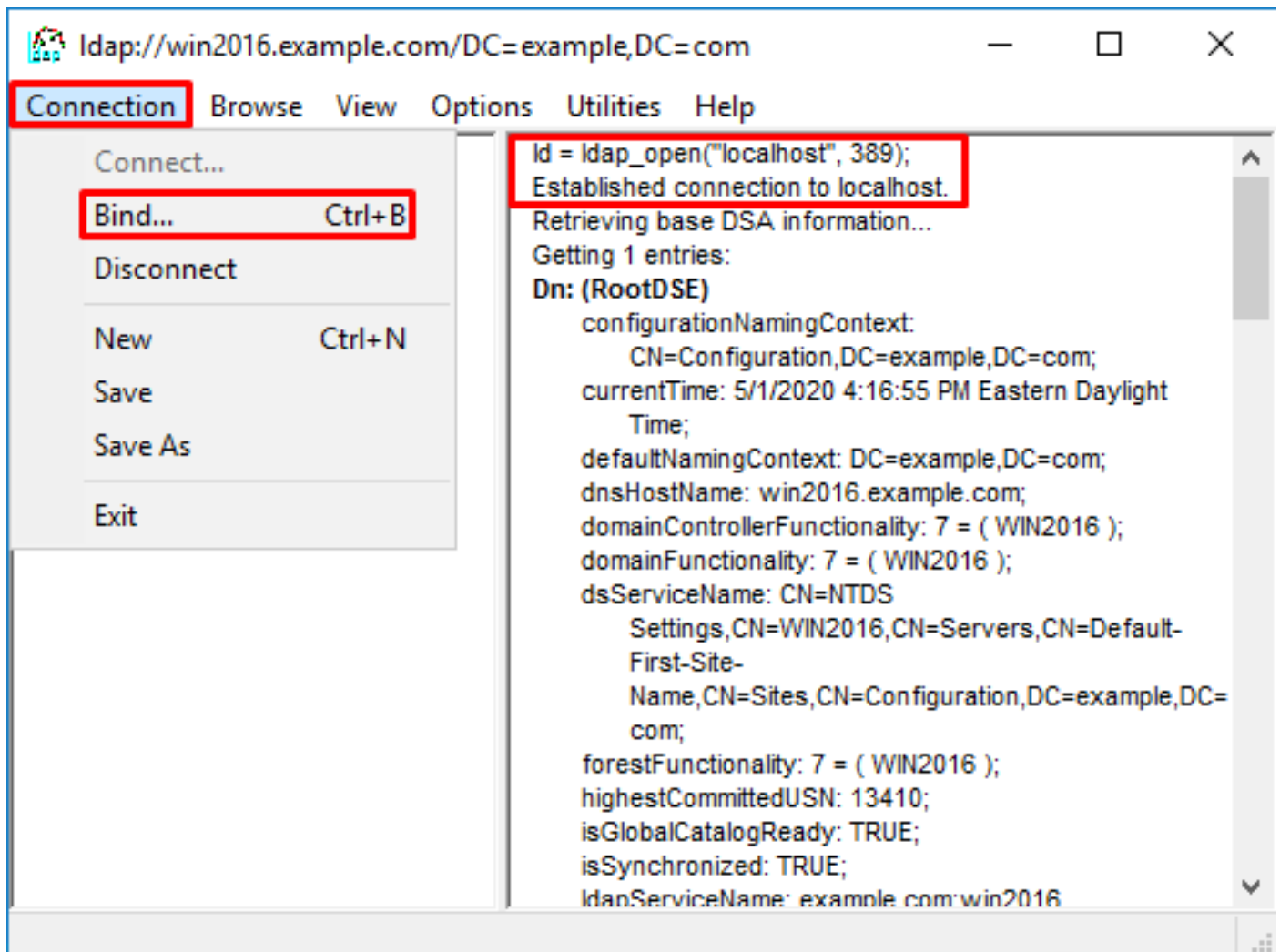
3. Especifique localhost para el servidor y el puerto adecuado y, a continuación, haga clic en Aceptar.



The image shows a 'Connect' dialog box with the following fields and options:

- Server:** localhost
- Port:** 389
- Connectionless
- SSL
- OK** (highlighted with a red border)
- Cancel**

4. La columna derecha muestra texto que indica una conexión correcta. Vaya a Conexión > Enlazar.



5. Seleccione Simple Bind y especifique el usuario de cuenta de directorio y la contraseña. Click OK.

Bind ✕

User: ftd.admin@example.com

Password: ●●●●●●●●

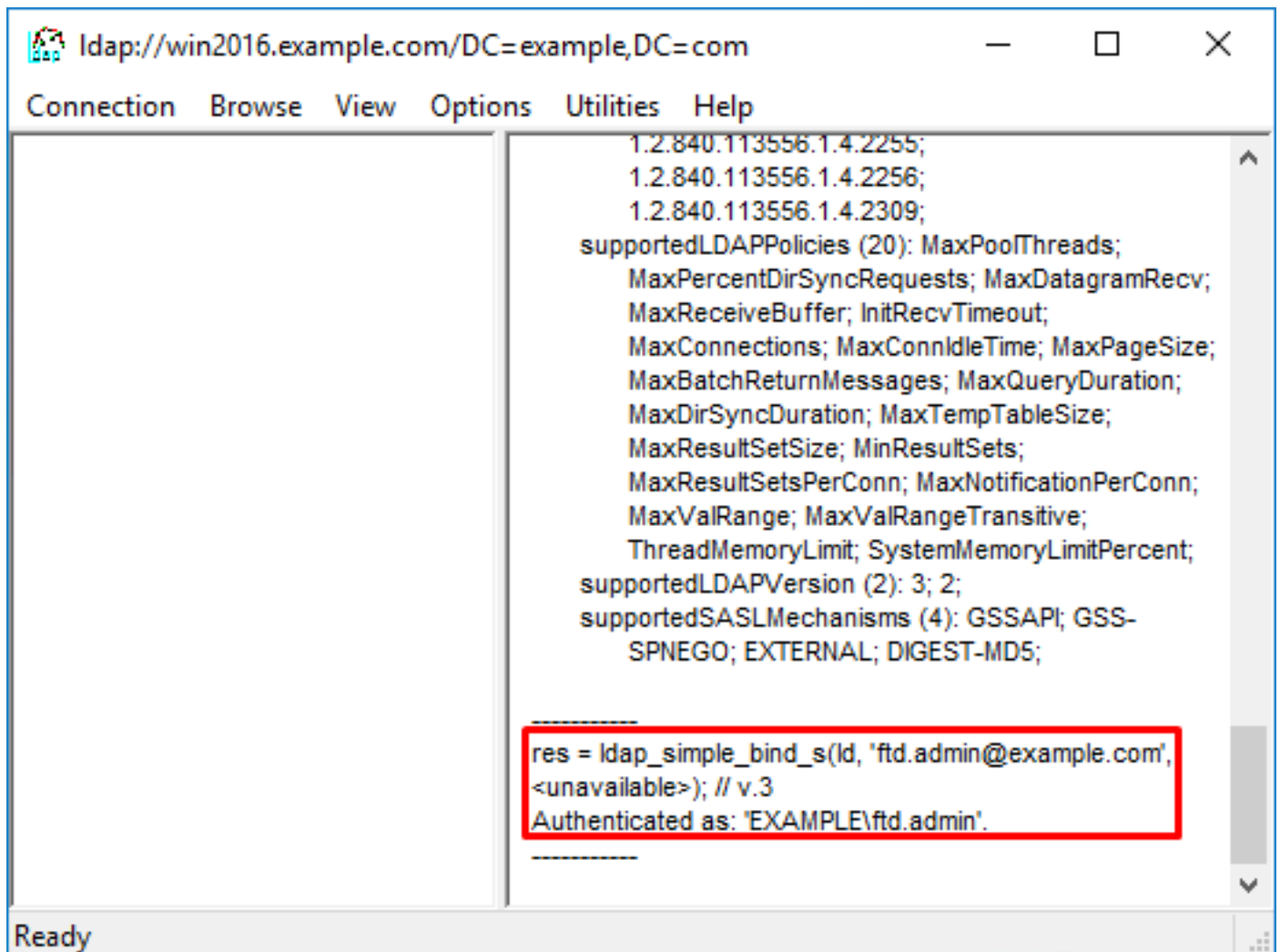
Domain:

Bind type

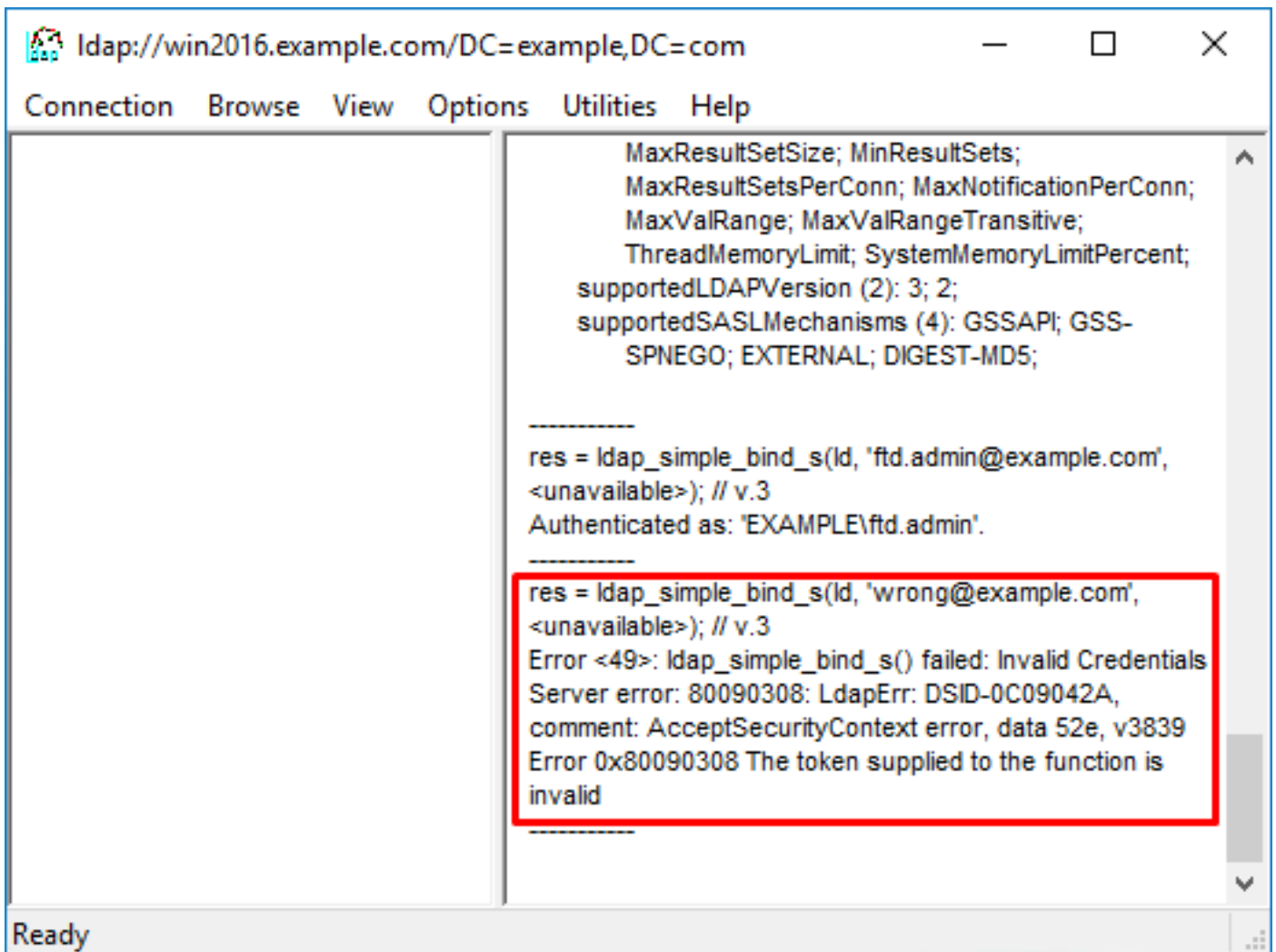
- Bind as currently logged on user
- Bind with credentials
- Simple bind
- Advanced (DIGEST)

Encrypt traffic after bind

Con un enlace exitoso, Idp muestra Authenticated as: DOMAIN\username



Si se intenta enlazar con un nombre de usuario o una contraseña no válidos, se producirá un error como los dos que se muestran aquí.



El servidor LDAP no puede encontrar el nombre de usuario

<#root>

```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] supportedLDAPVersion: value = 3
[-2147483612] supportedLDAPVersion: value = 2
[-2147483612] LDAP server 192.168.1.1 is Active directory
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] LDAP Search:
    Base DN = [dc=example,dc=com]
    Filter   = [samaccountname=it.admi]
    Scope    = [SUBTREE]
[-2147483612]

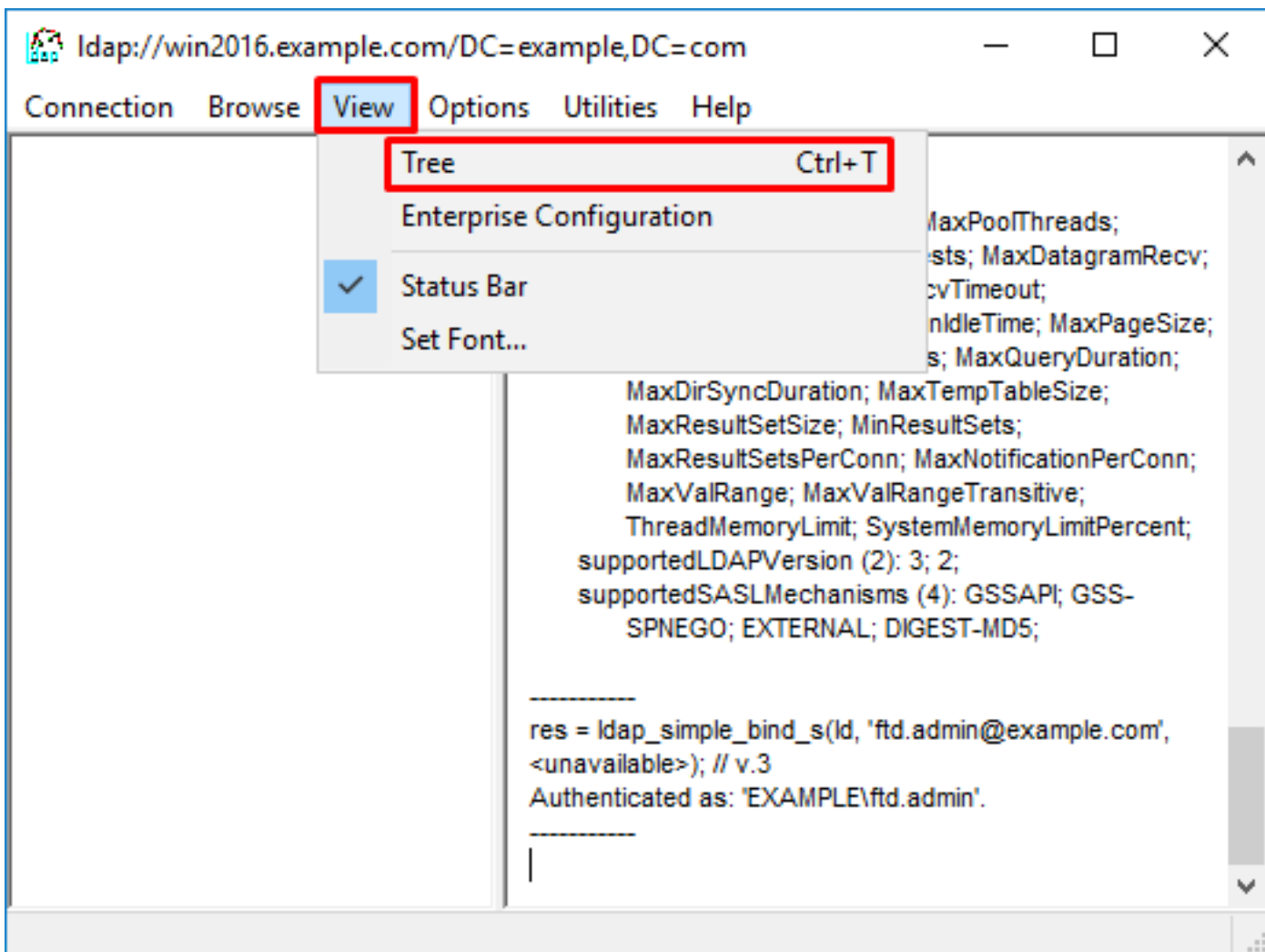
Search result parsing returned failure status

[-2147483612] Talking to Active Directory server 192.168.1.1
[-2147483612] Reading password policy for it.admi, dn:
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
```

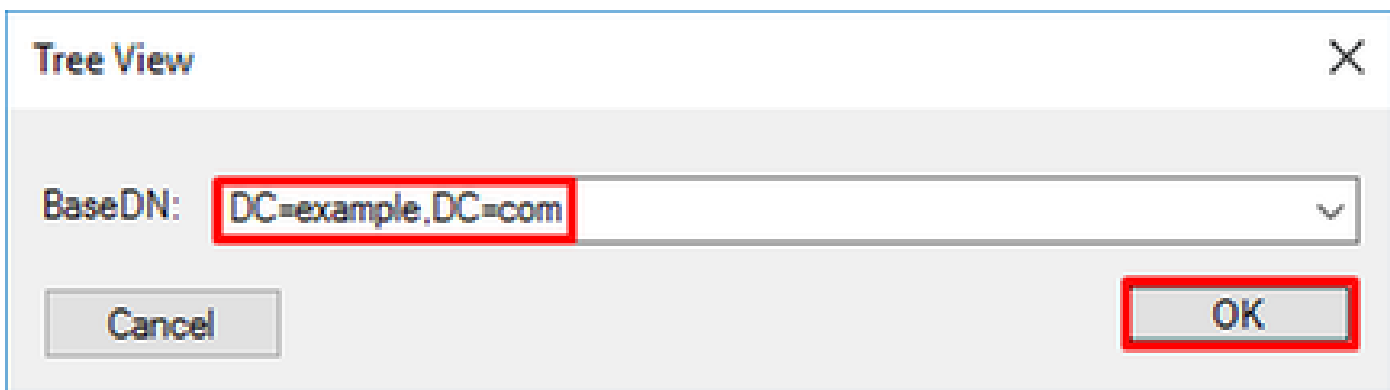
[-2147483612] Fiber exit Tx=456 bytes Rx=1082 bytes, status=-1
[-2147483612] Session End

Solución potencial: compruebe que AD puede encontrar el usuario con la búsqueda realizada por el FTD. Esto se puede hacer con ldp.exe también.

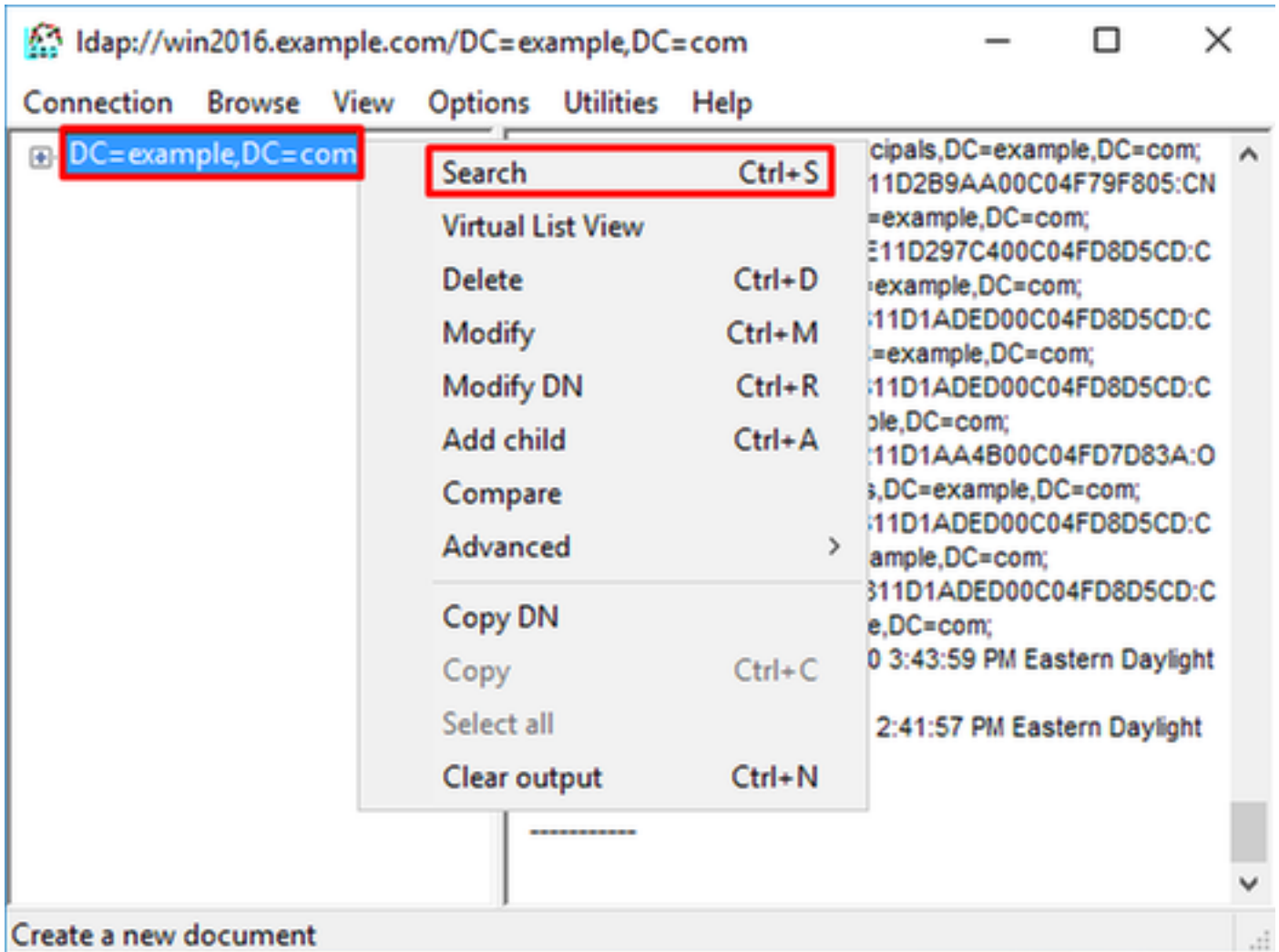
1. Después de enlazar correctamente como se ve arriba, navegue hasta Ver > Árbol.



2. Especifique el DN base configurado en el FTD y haga clic en Aceptar



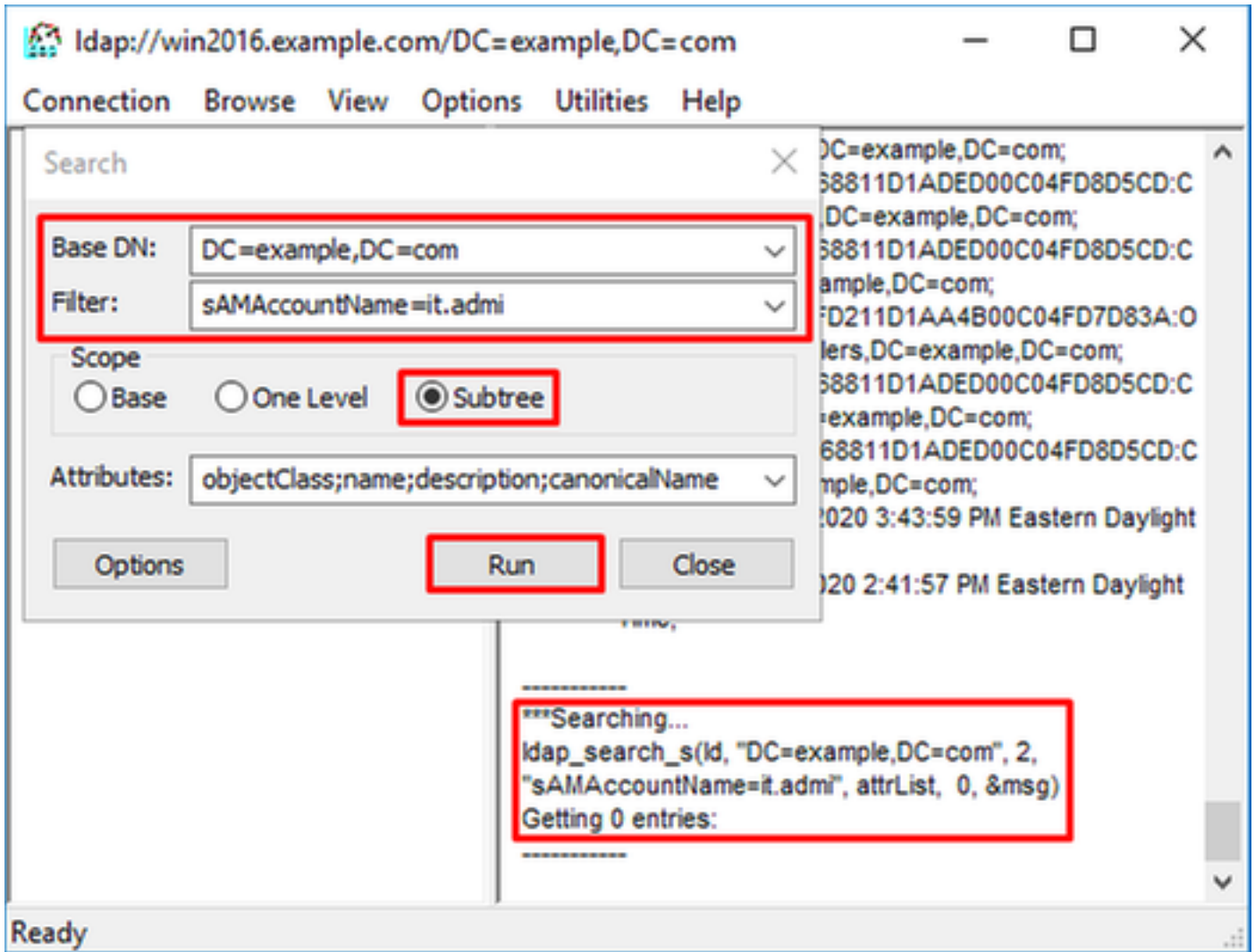
3. Haga clic con el botón derecho en el DN base y luego haga clic en Buscar.



4. Especifique los mismos valores DN base, Filtro y Ámbito que se ven en las depuraciones.

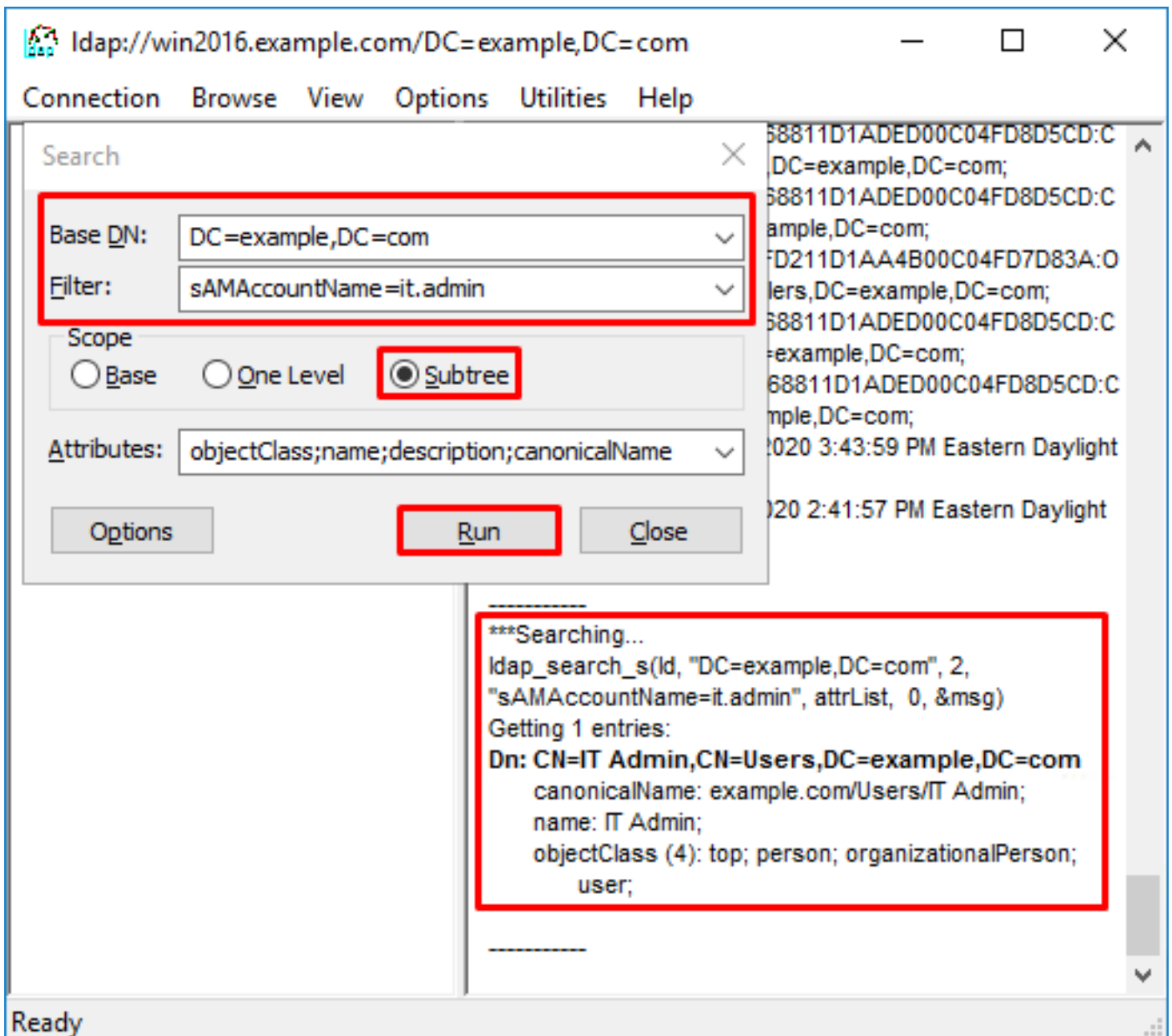
En este ejemplo, estos son:

- DN base: dc=ejemplo,dc=com
- Filtro: samaccount=it.admi
- Ámbito: SUBÁRBOL



Idp encuentra 0 entradas porque no hay ninguna cuenta de usuario con el sAMAccountName it.admi bajo el DN base dc=example,dc=com.

Otro intento con el sAMAccountName it.admin correcto muestra un resultado diferente. Idp encuentra 1 entrada bajo el DN base dc=example,dc=com e imprime ese DN de usuario.



Contraseña incorrecta para el nombre de usuario

<#root>

```

[-2147483613] Session Start
[-2147483613] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483613] Fiber started
[-2147483613] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483613] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483613] supportedLDAPVersion: value = 3
[-2147483613] supportedLDAPVersion: value = 2
[-2147483613] LDAP server 192.168.1.1 is Active directory
[-2147483613] Binding as ftd.admin@example.com
[-2147483613] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483613] LDAP Search:
      Base DN = [dc=example,dc=com]
      Filter  = [samaccountname=it.admin]
      Scope   = [SUBTREE]
[-2147483613] User DN = [CN=IT Admin,CN=Users,DC=example,DC=com]
[-2147483613] Talking to Active Directory server 192.168.1.1
  
```

```
[-2147483613] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[-2147483613] Read bad password count 0
[-2147483613] Binding as it.admin
[-2147483613] Performing Simple authentication for it.admin to 192.168.1.1
[-2147483613]
```

Simple authentication for it.admin returned code (49) Invalid credentials

```
[-2147483613] Message (it.admin): 80090308: LdapErr: DSID-0C09042A, comment: AcceptSecurityContext error
[-2147483613]
```

Invalid password for it.admin

```
[-2147483613] Fiber exit Tx=514 bytes Rx=2764 bytes, status=-1
[-2147483613] Session End
```

Posible solución: compruebe que la contraseña de usuario está configurada correctamente y que no ha caducado. Al igual que el DN de inicio de sesión, el FTD realiza un enlace con AD con las credenciales del usuario.

Este enlace también se puede hacer en ldp para verificar que AD pueda reconocer las mismas credenciales de nombre de usuario y contraseña. Los pasos en ldp se muestran en la sección DN de Login de Enlace y/o contraseña incorrecta.

Además, los registros del Visor de eventos de Microsoft Server se pueden revisar por un motivo de error potencial.

Prueba AAA

El comando test aaa-server se puede utilizar para simular un intento de autenticación del FTD con un nombre de usuario y una contraseña específicos. Esto se puede utilizar para probar fallos de conexión o autenticación. El comando es test aaa-server authentication [AAA-server] host [AD IP/hostname].

```
<#root>
```

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
  realm-id 7
aaa-server
```

LAB-AD

host

win2016.example.com

```
server-port 389
ldap-base-dn DC=example,DC=com
ldap-scope subtree
ldap-login-password *****
ldap-login-dn ftd.admin@example.com
server-type auto-detect
```

```
> test aaa-server authentication
```


LAB-AD

host

win2016.example.com

Username: it.admin

Password: *****

INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)

INFO: Authentication Successful

Capturas de paquetes

Las capturas de paquetes se pueden usar para verificar la disponibilidad al servidor AD. Si los paquetes LDAP dejan el FTD, pero no hay respuesta, esto podría indicar un problema de ruteo.

La captura muestra el tráfico LDAP bidireccional.

```
> show route 192.168.1.1
```

```
Routing entry for 192.168.1.0 255.255.255.0
```

```
Known via "connected", distance 0, metric 0 (connected, via interface)
```

```
Routing Descriptor Blocks:
```

```
* directly connected, via inside
```

```
Route metric is 0, traffic share count is 1
```

```
> capture AD interface inside match tcp any host 192.168.1.1 eq 389
```

```
> show capture
```

```
capture AD type raw-data interface inside [Capturing - 0 bytes]
```

```
match tcp any host 192.168.1.1 eq ldap
```

```
> test aaa-server authentication LAB-AD host win2016.example.com username it.admin password *****
```

```
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
```

```
INFO: Authentication Successful
```

```
> show capture
```

```
capture AD type raw-data interface inside [Capturing - 10905 bytes]
```

```
match tcp any host 192.168.1.1 eq ldap
```

```
> show capture AD
```

```
54 packets captured
```

```
1: 23:02:16.770712      192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win 32768 .
2: 23:02:16.772009      192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack 36819128
3: 23:02:16.772039      192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768 <nop,nop,ti
4: 23:02:16.772482      192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145) ack 4915
5: 23:02:16.772924      192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack 368191
6: 23:02:16.772955      192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768 <nop,nop,ti
7: 23:02:16.773428      192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44) ack 49152
8: 23:02:16.775030      192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack 3681913
9: 23:02:16.775075      192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768 <nop,nop,ti
```

```
[...]
```

```
54 packets shown
```

Registros del Visor de sucesos de Windows Server

Los registros del Visor de eventos en el servidor de AD pueden proporcionar información más detallada sobre el motivo de un error.

1. Busque y abra el Visor de sucesos.



Best match



Event Viewer

Desktop app

Settings



View event logs



Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).